Comments of

TechFreedom

National Telecommunications & Information Administration (NTIA)

Request for Comment (RFC), 83 Fed.Reg. 48600 (September 26, 2018)

Berin Szóka & James Dunstan[i]

[i] Berin Szóka (bszoka@techfreedom.org) is President of TechFreedom, TechFreedom (techfreedom.org), a nonprofit, *nonpartisan* technology policy think tank. James Dunstan (jdunstan@techfreedom.org) is General Counsel of TechFreedom.org. This document could not have been completed without the assistance of Alvaro Marañon, Legal Intern at TechFreedom and a law student at American University Washington College of Law.

Executive Summary

We commend the NTIA for conducting this inquiry as an essential step towards bringing the heated "privacy" debate towards consensus. The Request for Comment (RFC) starts at the correct point, in asking about basic principles that should guide policy discussions, rather than suggesting a framework based on under-defined perceived problems, whether legitimate or not.

The NTIA's efforts are also supported by nearly a decade of work by the Department of Commerce, and a myriad of academics and stakeholders. TechFreedom has been deeply engaged in this issue since at least 2012. The 2012 Obama Framework, while it has some fundamental flaws, offers a useful starting point as a distillation of the American approach to consumer privacy.

How we think about privacy is a vital first step. First, it is not a single concept, but rather a multidimensional concept that looks different, depending on what angle you look at it. Second, "privacy" is not synonymous with a property right. While there may be legitimate property rights that can be associated with data that can impact privacy, privacy itself is not a property right, as property-tizing personal information is virtually unworkable in practice.

If instead of focusing on fundamental principles, NTIA jumps immediately to suggesting solutions to perceived privacy problems, the result could well be a recommendation to adopt policies that in many way mirror either Europe's General Data Protection Regulation (GDPR), or the recent California Consumer Privacy Act of 2018 (CCPA). As we discuss below, both approaches are flawed in fundamental respects. Adopting a GDPR-regime in the United States would ignore two hundred years of American law and jurisprudence related to the concept of privacy as an adjunct to the concept of fundamental liberty. It also would ignore the significant existing statutory regimes Congress has established concerning certain types of data and certain privacy rights that should not be replaced, but rather harmonized in any top level federal privacy policy.

The CCPA can best be described as half-baked sausage. This rushed piece of state legislation contains 10,000 words of inconsistency, undefined terms, and potential traps for businesses, including significant civil fines and class action statutory damages—all without the benefit of a full record of defining fundamental principles of privacy. Given the inherently interstate nature of data travelling on the Internet, such a state law that conflicts with federal policy (and especially future federal statutes), may be unconstitutional and deserved to be preempted by Federal legislation.

Another principle mentioned neither by the GDPR (because it doesn't apply), or California (because it was simply ignored), is the important role that the First Amendment must play in any privacy analysis. The NTIA should look to the well-developed jurisprudence related to the applicability of the First Amendment first to commercial speech, then to commercial data, in establishing first principles. The right to reach out to people and "speak" to them based on inferences about their likely interests, whether the subject is politics or fishing polls, is protected under the Constitution, and we can't simply throw that aside in favor of a new "super" right called privacy.

How then, should we consider the mechanisms to protect privacy? This requires analyzing the administrative law framework, which agency will be "on the watch," and what their enforcement tools should be. If the FTC is to be the "cop on the beat," are its current tools sufficient under notions of "unfairness" and "deception"? What type of deference and judicial review should apply to the FTC's efforts to protect consumer privacy? What burdens of proof should apply to parties engaged in a dispute as to whether a party failed to adequately protect the privacy of an individual or their data? Can the FTC establish a "one size fits all" data protection policy that can apply equally to a Fortune 100 company in the same way it applies to a small vendor selling items on eBay?

And how should the FTC establish the norms for privacy and data security and ensure that all users of the Internet have fair notice of these policies? Are all businesses collecting and exchanging data on the Internet charged with reading every FTC Consent Decree, FAQ and the transcripts of FTC workshops to divine the standard of care required to protect the privacy of people they deal with on the Internet? Is the risk of a data breach for a company with 1,000 records the same as a data breach for a company with 100,000,000 data files?

What are the proper roles for state attorneys general and private rights of action? Are there dangers of differential enforcement based on politics? Is creating a cottage industry of class action lawyers an efficient and effective tool to protect consumer privacy?

We address many of these issues in the comments below, as well as comment on a number of the specific principles proposed in the RFC. But we recognize that these comments, and the comments of other stakeholders, can only be the beginning of this discussion. That is why we strongly endorse the establishment of a Privacy Law Modernization Commission, modeled after the 1970 expert commission that originally developed the Fair Information Practice Principles and the Antitrust Modernization Commission established by Congress in 2002. Such a commission should be directed to move swiftly to study the issues and issue a preliminary report. With the January 1, 2020 implementation date of the CCPA, time is of the essence to bring all interested parties to the table to debate these principles and reach consensus, or at least articulate where there are fundamental differences.

TechFreedom looks forward to continuing this dialog. Attached as appendices are:

A. Berin Szóka, Graham Owens, & Jim Dunstan, *Hearings on Competition & Consumer Protection in the 21st Century* (June 2018)
B. Berin Szóka & Graham Owens, Testimony of TechFreedom, *FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare*, Hearing before U.S. Senate, Committee on Commerce, Science, & Transportation (Sept. 26, 2017)
C. Berin Szóka & Geoffrey A. Manne, *The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature* (May 2016)
D. Brief of International Center for Law & Economics & TechFreedom as Amici Curiae Supporting Petitioners, *LabMD, Inc. v. Federal Trade Commission*, at 30-31 (11th Cir. Jan. 3, 2017)
E. Lothar Determann, *No One Owns Data*, UC Hastings Research Paper No. 265 (last updated Feb. 14, 2018)
F. Larry Downes, *A Rational Response to the Privacy 'Crisis'*, The Cato Institute, Policy Analysis #716 (Jan. 7, 2013)
G. Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 2 (1999)

Table of Contents

I. Introduction

We commend the NTIA for conducting this inquiry as an essential step towards bringing the heated "privacy" debate towards consensus. TechFreedom has been deeply engaged in this issue since at least 2012.[1] The Commerce Department, under President Obama's leadership, began a process like this over nine years ago, seeking comment from stakeholders in 2009, publishing a "Privacy and Innovation Notice of Inquiry" in April 2010, which led to a Green Paper issued in December 2010.[2] In 2012, based on that Green Paper, President Obama's White House released its "Consumer Privacy Bill of Rights."[3] TechFreedom observed, in testimony before the House Energy & Commerce Committee on that document, that:

> The central challenge facing policymakers on privacy is three-fold:
>
> 1. Defining what principles should govern privacy policy;
>
> 2. Transposing those principles into concrete rules, whether through self-regulation or legislation, and updating them as technology changes; and
>
> 3. Determining how to effectively enforce compliance.

---

[1] Berin Szóka, Graham Owens, & Jim Dunstan, *Hearings on Competition & Consumer Protection in the 21st Century* (June 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0049-d-2147-155147.pdf (hereinafter *2018 TechFreedom FTC Comments*);Berin Szóka & Graham Owens, Testimony of TechFreedom, *FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare*, Hearing before U.S. Senate, Committee on Commerce, Science, & Transportation (Sept. 26, 2017), http://docs.techfreedom.org/Szoka_FTC_Reform_Testimony_9-26-17.pdf (hereinafter *2017 FTC Testimony*); Berin Szóka & Geoffrey A. Manne, *The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature* (May 2016), https://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf (hereinafter *2016 FTC Reform Report*); Geoffrey A. Manne, R. Ben Sperry & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1 (2015)(hereinafter *Nomi Paper*); Comments of Berin Szóka to the National Telecommunications and Information Administration on the Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct (Apr. 12, 2012), http://docs.techfreedom.org/Comments_NTIA_Multistakeholder_4.12.12.pdf; Testimony of Berin Szóka, House Energy & Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?* (March 29, 2012), http://techfreedom.org/wp-content/uploads/2018/08/Szoka-Testimony-at-House-Balancing-Privacy-and-Innovation.pdf.

[2] Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2011), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

[3] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* (Feb. 23, 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (hereinafter *CPBR*); *see also* White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (Feb. 27, 2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (hereinafter *2015 CPBR Legislation*).

> Unfortunately, the privacy debate has until now focused mostly on the first part, crafting the right principles.[4]

But, as we noted, "the value of privacy principles depends on their transposition into real-world guidelines,"[5] enforcement, and compliance.

Now, this inquiry begins at the same place: seeking feedback on modified versions of the seven high-level principles put forth in 2012.[6] The similarity between the 2012 principles and the principles now proposed by NTIA — as reflected in the chart that follows[7] — reflects a high-level consensus regarding the American approach to privacy, largely distilled from the Federal Trade Commission's case-by-case enforcement over nearly the last two decades. The seemingly differences between the two sets of principles are important (*e.g.*, focusing on context versus risk), as we discuss below.

Ultimately, however, what is even more important is how such principles are to be operationalized in the real-world. That, in turn, requires having a framework for understanding how law will operate in this arena. It is on these questions of administrative and constitutional law that our comments focus. Our goal is to help policymakers understand both how to craft their principles, based on how they might be put into practice, and also to shape what is to us the more important conversation in the long-term: When are rules appropriate rather than standards? Who should bear burdens of proof? What role should evidentiary presumptions play? How much detail do data processors need to be given constitutionally required "fair notice" of what the law requires? When is such detail counter-productive? What enforcement tools should be used when? When are civil penalties appropriate, and when should enforcement continue to focus, as the FTC does today under Section 5, on injunctive and remedial relief? How will the First Amendment shape restrictions on the use, collection and sharing of information?

The American approach to governing the collection, use and sharing of personal information through flexible, case-by-case enforcement based largely on the generally applicable standards of consumer protection law, and partly on a series of laws focused on specific harms (*e.g.*, children's privacy, health information, financial information) has allowed American

---

[4] Comments of TechFreedom to the Nat'l Telecomm. & Info. Admin. (NTIA), *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*, at 2 (April 2, 2012), available at http://docs.techfreedom.org/Comments_NTIA_Multistakeholder_4.12.12.pdf.

[5] *Id.* at 3.

[6] Press Release, NTIA, *NTIA Seeks Comments on New Approach to Consumer Data Privacy,* Sept. 25, 2018, https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy (hereinafter *RFC*).

[7] *See infra* at 9.

companies to take unquestioned leadership in the tech sector, globally. Policymakers should take the greatest care in overhauling that system, lest they choke a virtuous cycle of innovation that has delivered so may benefits to Internet users around the world.

It is perfectly appropriate to update the current FTC approach to privacy by codifying (or even modifying) specific aspects of existing practice into legislation. The history of American consumer protection law is essentially one of that process: The Federal Trade Commission develops law in an area, and Congress occasionally supplements that law with statutory codification. But in doing so, Congress has always focused on one specific area at a time. This approach has been derided as a patch-work, but in fact, it reflects a well-deserved humility about the ability of policymakers to accurately weigh the tradeoffs inherent in restricting the use and collection of a particular data in a particular context.

II. How to Think about Privacy

How we talk about "privacy" has profound consequences for our ability to craft workable policy. We begin by addressing two conceptual pitfalls that plague this debate: (1) the tendency to think of "privacy" as a single concept and (2) the tendency, both among the most vocal "privacy" advocates and also many who tend to think about the world in terms of markets, to conceive of "privacy" in terms of property rights.

A. A Vast, Sprawling & Diverse Continent of Concerns

Any conversation about "privacy" often begins from a false rhetorical premise: that "privacy" is a single problem, or even a family of problems that share the same essential characteristic. As Prof. Daniel Solove has argued, privacy is best understood as a cluster of issues that share "family resemblances," to borrow the concept of the philosopher Ludwig Wittgenstein.[8] Solove argues:

> Trying to solve all privacy problems with a uniform and overarching conception of privacy is akin to using a hammer not only to insert a nail into the wall but also to drill a hole. Much of the law of information privacy was shaped to deal with particular privacy problems in mind. The law has often failed to adapt to deal with the variety of privacy problems we are encountering today. Instead, the law has attempted to adhere to overarching conceptions of privacy that do not work for all privacy problems. Not all privacy problems are the same, and different conceptions of privacy work best in different contexts. Instead of trying to fit new prob-

[8] Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087, 1096-99 (2002).

> lems into old conceptions, we should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption? How does this disruption affect society and social structure?[9]

Solove argues for privacy pragmatism:

> A pragmatic approach to the task of conceptualizing privacy should not, therefore, begin by seeking to illuminate an abstract conception of privacy, but should focus instead on understanding privacy in specific contextual situations…
>
> the pragmatist has a unique attitude toward conceptions. Conceptions are "working hypotheses," not fixed entities, and must be created from within concrete situations and constantly tested and shaped through an interaction with concrete situations.[10]

This is exactly the right way to begin thinking about privacy — rather than beginning from the premise that "privacy is a right," which presumes both that "privacy" is a single thing, and that a framing based on rights makes sense. Solove continues:

> The problem with discussing the value of privacy in the abstract is that privacy is a dimension of a wide variety of practices each having a different value—and what privacy is differs in different contexts. My approach toward conceptualizing privacy does not focus on the value of privacy generally. Rather, we must focus specifically on the value of privacy within particular practices.[11]

In general, addressing concerns about privacy in a dynamic world requires weighing competing values in specific situations — which, as discussed below, is generally best done through the application of standards case-by-case, rather than by attempting to deduce all the logical consequences of first premises of privacy law and codify those into rules.

B. The Limits of the Property Rights Analogy

Faced with the complexity of "privacy" — the continental scale of the problem — many naturally want to reduce the issue to the comfortable, familiar metaphor of property rights. We attach hereto two papers by Internet legal scholars explaining the unsuitability of the property rights analogy to data.

---

[9] *Id.* at 1146-47.

[10] *Id*. at 1128-29.

[11] *Id.* at 1146.

As privacy lawyer Lothar Determann notes, even some of the strongest advocates of privacy as a property right have found the idea unworkable in practice:

> EU lawmakers have taken broad action to protect data privacy and have restated in the new General Data Protection Regulation (GDPR) that companies are generally prohibited from processing any personal data unless there is a statutory exception. Such strongly worded exclusion rights have been likened to property law concepts. Yet, GDPR stops short of recognizing ownership or property rights for data subjects and refers to "ownership" and "property" only to recognize the conflicting rights that may outweigh privacy interests. Even the novel right to data portability is quite limited: it applies only to personal data provided (not: created or acquired by an "owner"), by the data subject (not: any "owner"), based on consent or contract (not: legitimate interests, law or other bases), and does not confer any exclusion, usage or alienation rights.[12]

Author Larry Downes likewise rejects the analogy to property rights in his 2013 paper for the Cato Institute,

> The property rights solution is elegant and logical: assign property rights to consumers for personally identifiable information, then give them the tools to manage and enforce those rights, including, if they like, to sell them. If a coalition of government agencies and responsible corporate users can get together and establish enforceable property rights over private information, anarchy will subside. Emotion disappears; problem solved.[13]
>
> …
>
> We cannot solve the privacy "crisis" by treating information as the personal property of those to whom it refers or by adapting the systems for protecting copyright, patent, and other so-called "intellectual property" to personal information. But a related body of law explains and rationalizes what is going on with personal information and privacy: the more flexible solution of information licensing. The licensing model recognizes that most information with economic value is the collaborative creation of multiple sources, including individuals and service providers. Rather than establish enforceable title to property, it assumes joint ownership and licenses specific uses based on mutual exchange of value[14]

---

[12] Lothar Determann, *No One Owns Data,* UC Hastings Research Paper No. 265 (last updated Feb. 14, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123957.

[13] Larry Downes, *A Rational Response to the Privacy 'Crisis'*, The Cato Institute, Policy Analysis #716, at 7 (Jan. 7, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200208.

[14] *Id*. at 1.

Downes explains the various problems with the property analogy,[15] but the most salient discussion is this:

> Another objection to the ownership approach is its unexplored assumption that the initial allocation of a property right should go to the individual to whom the information refers. That starting point isn't obvious. While the information we are talking about refers to or describes a particular person, that does not mean that the person actually exerted any effort to create the information, or that they have done anything to make it useful in combination with the information of other individuals. You spend money, accept credit, and pay your bills, but that doesn't mean you've done anything to make a useful record of your credit history future lenders can evaluate.
>
> So we might instead think that those who unearth, normalize, store, and process information ought to be the initial owners of any property rights to it. For one thing, they need the economic incentive. Why else would a company go to the trouble of collecting various public and private records of your payment, employment, and asset history in order to create a credit profile? Under the view of Lessig and others, the moment that profile was of any value, its ownership would be assigned to the individual to whom it refers.
>
> If that were the property rights system for privacy, no for-profit entity would bother to create credit profiles, which require not only an individual's information but the ability to compare it to the information of large groups of similar and dissimilar consumers. And unless you live your life paying cash for everything, you need someone to compile that history. Otherwise, there's no basis for a lender to determine the appropriate risk for a loan. Your lender will either make no loans or charge exorbitant interest rates. This is a central defect in Lessig's assumption and the less sophisticated claim by some privacy advocates that you "own" information simply because it refers to you.[16]

(Downes goes on to examine the initial allocation of rights through the work of Ronald Coase, the economist whose work has shaped essentially all modern thinking about property law.) As discussed below, the only area in which a property rights analogy makes some sense (and even then, has real limits) is in the context of information we actively provide about ourselves (such as the private emails we write or photos we might upload), as opposed to information that is observed about us.[17]

---

[15] *Id.* at 17-25.

[16] *Id*. at 18.

[17] *See infra* at 39 *et seq*.

III. NTIA's Proposed Principles in Context

NTIA's proposed principles must be considered in comparison with three other legislative frameworks: (1) the Obama Administration's 2012 proposed framework, as further implemented in proposed 2015 legislation; (2) the European Union's General Data Protection Regulation (GDPR); and (3) the California Consumer Privacy Act.

A. Comparison to the 2012 Obama Framework

The easiest way to understand and evaluate NTIA's proposed principles is to compare them with the seven mostly analogous principles contained in the Consumer Privacy Bill of Rights proposed by the Obama Administration in 2012, as this chart indicates. For the most part, the differences in wording are differences in framing: the 2012 Obama document framed each concept as a right, while the NTIA's principles focus on outcomes for consumers.

Concepts	2012 CPBR	2018 NTIA
Individual control	Consumers have a right to exercise control over what personal data companies **collect** from them and how they use it.	Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they **provide** to organizations.
Transparency	Consumers have a right to easily understandable and accessible information about privacy and security practices.	Organizations should be transparent about how they collect, use, share, and store users' personal information.
Respect for Context	Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the **context** in which consumers provide the data.	Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the **context** and **risk** of privacy harm
Security	Consumers have a right to secure and responsible handling of personal data	Organizations should employ security safeguards to protect the data that they collect, store, use, or share.
Access and Accuracy	Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.	Users should be able to reasonably access and correct personal data they have **provided**.
Collection Management	Consumers have a right to reasonable limits on the personal data that companies collect and retain	Organizations should take steps to manage the risk of disclosure or harmful uses of personal data.
Accountability	Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.	Organizations should be accountable for the use of personal data that has been collected, maintained or used by its systems

B. Why Europe's GDPR Is a Poor Model for the U.S.

Some in Congress have argued that the U.S. should implement some or all of the European Union's General Data Protection Regulation (GDPR).[18] We believe that would be a profound mistake.

First, it must be understood that the EU process that led to the GDPR was, and the resulting regulation is, much more about data governance than privacy protection. "A popular misconception about the GDPR is that it protects privacy; in fact, it is about data protection or, more correctly, data governance."[19] There is a significant difference between the two.

> The International Association of Privacy Professionals (IAPP) Glossary notes that data or information privacy is the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." Data protection, on the other hand, is the safeguarding of information from corruption, compromise, or loss. IPSwitch summarizes the difference: "data protection is essentially a technical issue, whereas data privacy is a legal one.[20]

This different approach comes from a very different history of privacy protection and cultures between Europe and the United States. This country has recognized the right of privacy since the Bill of Rights. "The American notion of privacy is predicated in large part on freedom from government intrusion and as a counterweight to the growth of the administrative state."[21] The U.S. already has a number of privacy statutes that did not exist in the EU prior to GDPR, and an existing agency (the FTC) with 100 years of protecting consumers, not a brand new super directorate just learning how to walk. These privacy statutes include, but are in no way limited to: the Privacy Act of 1974,[22] the Gramm-Leach-Bliley Act,[23] the Fair

---

[18] See Press Release, Senator Ed Markey, Senator Markey Introduces Resolution to Apply European Privacy Protections to Americans, (May 24, 2018), https://tinyurl.com/y9xawr9c; Press Release, Senator Ed Markey, As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights, (April 10, 2018), https://tinyurl.com/ybnghj6v.

[19] R. Layton & Julian Mclendon, *The GDPR: What is Really Does and How the U.S. Can Charter a Better Course*, 19 The Federalist Society Review 234, 235 (2018), https://fedsoc-cms-public.s3.amazonaws.com/update/pdf/nv29MXryrqablN7n8h6WzAJ9yhbZBKITKOMwMzVe.pdf (hereinafter What GDPR Does).

[20] *Id*. at 235, citing: Information Privacy, Glossary, IAPP https://iapp.org/resources/glossary/#information-privacy; David Robinson, *Data Privacy vs. Data Protection*, IPSwitch (Jan. 29, 2018), https://blog.ipswitch.com/data-privacy-vs-data-protection.

[21] What GDPR Does, *supra* note 19, at 236.

[22] 5 U.S.C. § 552a.

[23] 15 U.S.C. §§ 6801-6809.

Credit Reporting Act,[24] the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[25] the Freedom of Information Act (FOIA),[26] and the Children's Online Privacy Protection Act (COPPA).[27]

There are significant cultural differences between the U.S. and EU countries which colors the debate about the individual's right to privacy versus the public's right to know.[28] Some have argued that it boils down to "permissionless innovation" versus "the precautionary principle."[29] The definition of what constitutes private information is very different in the U.S. than in EU countries. For example, Nordic countries make salary information and income tax filings and other sensitive financial information available to the public, whereas those documents are protected under U.S. law from public release.[30] Conversely, the EU protects criminal records, while the U.S. has a public policy of allowing the public access to criminal records.[31]

Early implementation of the GDPR and the fall-out from it, should caution the NTIA from using GDPR as a model. The GDPR's reliance on "the precautionary principle" has resulted in a complex and horrifically expensive set of regulations that have already produced negative and innovation crushing results. We are aware of one small U.S. computer game company

---

[24] 15 U.S.C. § 1681 et seq.

[25] 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.

[26] 5 U.S.C. § 552.

[27] 15 U.S.C. §§ 6501–6505.

[28] What GDPR Does, *supra* note 19, at 237.

[29] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, Mercatus Center, available at https://www.mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom. Thierer submits that the precautionary principle is the belief that "innovations should be curtailed or disallowed until their developers can prove they will not cause any harm to individuals, groups, specific entities, cultural norms, or various existing laws, norms or traditions," and contrasts it with permissionless innovation, in which "experimentation with new technologies and business models should be generally permitted by default"; *see also* Adam Thierer, *Embracing a Culture of Permissionless Innovation*, Cato Institute (Nov. 17, 2014), https://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.).

[30] What the GDPR Does, *supra* note 19, at 237, *citing Tax Statistics for Personal Tax Payers*, Statistisk Sentralbyrå, Apr. 18, 2018, https://www.ssb.no/en/inntekt-og-forbruk/statistikker/selvangivelse/aar-forelopige/2018-04-18; Patrick Collinson, *Norway, the Country Where You Can See Everyone's Tax Returns*, The Guardian (Apr. 11, 2016), https://www.theguardian.com/money/blog/2016/apr/11/when-it-comesto-tax-transparency-norway-leads-the-field; *Income and Tax Statistics in Sweden*, Statistiska Centralbyrån, Oct. 1, 2018, http://www.scb.se/en/finding-statistics/statistics-by-subject-area/household-finances/ income-and-income-distribution/income-and-tax-statistics/.

[31] *Id.*, *citing* James Jacobs and Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records,* 11 N.Y.U. J. L. & Pub. Pol'y 177 (2012), http://www.nyujlpp.org/wp-content/uploads/2012/10/Jacos-Crepet-The-Expanding-Scope-Use-and-Availability-of-Criminal-Records.pdf.

(with a team of less than 20), with European players, which collected almost no private data (as defined under the GDPR), that had to expend over 450 person-hours to implement the GDPR.[32] Other U.S. companies have chosen to quarantine off Europe and stop doing business there.[33]

Most concerning about the GDPR is the powerful private rights of action by which it could be enforced. "[T]he statute itself suggests another set of stakeholders: litigants, non-profit organizations, data protection professionals, and data regulatory authorities. Non-profit organizations are empowered with new rights to organize class actions, lodge complaints, and receive compensation from fines levied on firms' annual revenue, as high as four percent of annual revenue."[34] It took just a matter of days before European lawyers spooled up to file class actions, claiming breaches of the GDPR. "Just seven hours after the European Union's General Data Protection Regulation (GDPR) came into effect on May 25, 2018, Austrian activist Max Schrems' non-profit None of Your Business (NOYB) lodged four complaints with European data protection authorities (DPAs) against Google and Facebook, claiming that the platforms force users' consent to terms of use and demanding damages of $8.8 billion. Soon after, the French advocacy group La Quadrature du Net (LQDN) filed 19 complaints, gathering support from its "Let's attack GAFAM and their world" campaign with a declared objective to "methodically deconstruct" Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) and their 'allies in press and government.'"[35] With the "low hanging fruit" of damages equaling up to four percent (4%) of gross revenues, an American-styled GDPR would open the floodgates on a wave of class action suits that would make wave of class actions under the Telephone Consumer Protection Act (TCPA) look like a trickle.[36]

The GDPR also vests enormous power in new state agencies to interpret and enforce the vague provisions of the GDPR. "The 29 [data protection authorities] across the 28 member nations are charged with 35 new responsibilities to regulate data processing."[37] Whether

[32] At a blended cost of management, senior engineers and outside legal counsel of $200 per hour, this very small company expended the equivalent of $90,000 to become GDPR compliant.

[33] "[T]housands of online entities, both in the EU and abroad, have proactively shuttered their European operations for fear of getting caught in the regulatory crosshairs." What the GDPR Does, *supra* note 19, at 234-5.

[34] What GDPR Does, *supra* note 19, at 234.

[35] *Id*.

[36] *See* "TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits," U.S. Chamber Institute for Legal Reform, (Aug. 31, 2017), https://www.instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits.

[37] What the GDPR Does, *supra* note 19, at 234.

these DPAs are up to the task of regulating and enforcing the elaborate construct of the GDPR remains to be seen.[38]

In short, NTIA should learn from the failings of the GDPR in the following areas:

1. Focus on privacy protection and not d`ata regulation;
2. Build upon 200 years of U.S. privacy protection policies and laws, not create new bureaucracies out of whole cloth that can be "weaponized" for political purposes;
3. Find solutions that encourage innovation, not shutter parts of the Internet; and
4. Limit private rights of action to truly egregious privacy breaches instead of creating a cottage industry of plaintiff class action lawyers.

C. California's CCPA

Another misguided "model" for federal privacy legislation would be the recent California Consumer Privacy Act of 2018 (CCPA), which is to take effect on January 1, 2020.[39] Even putting aside the problematic issue of states attempting to regulate the inherently interstate, indeed, international medium that is the Internet,[40] and whether new federal privacy legislation would preempt the CCPA, if we learn nothing else from the CCPA, it is that hastily drafted legislation that is over 10,000 words long is bound to result in complex interpretative issues that the courts will have to sort through for decades.[41] Some of the complexities introduced by the CCPA include:

1) There is no internal harmonization of existing California privacy laws. CCPA is just thrown on top like a heavy blanket, with somewhat bizarre "saving" language, including a statement that in the case of any conflicts with other California laws, the law that

[38] *See* Douglas Busvine et al., *European Regulators: We're Not Ready for New Privacy Law*, Reuters (May 8, 2018), https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X ("Seventeen of 24 authorities who responded to a Reuters survey said they did not yet have the necessary funding, or would initially lack the powers, to fulfill their GDPR duties").

[39] AB375, Title 1.81.5, adding Sections 1798.100 *et seq.*, signed into law June 28, 2018.

[40] *See generally* Graham Owens, White Paper, *Federal Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail*, at (July 19, 2018), at 56 http://dx.doi.org/10.2139/ssrn.3216665

[41] *See, generally*, Lothar Determann, *Broad data and business regulation, applicable worldwide,* International Association of Privacy Professionals (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

affords the greatest privacy protection shall control.[42] Similarly, the CCPA instructs courts that the new law "shall be liberally construed to effectuate its purposes."[43]

2) The definition of "personal information" is extremely broad, including the mere collection of IP addresses from website visits, and including any information that can be associated with a household, even if it can't be associated directly with an individual.[44]
3) Any company that collects any "personal information" about a California resident (including California residents that may be travelling outside the state), must comply if any of the three provisions below apply:
    a. The company has more than $25 million in "annual gross revenues;"
    b. The company obtains personal information of at least 50,000 California residents. This means that even small website operators will need to take steps to determine, to the extent they can, the geographic location of all visitors to their websites in order to determine whether they've met the 50,000 "trigger" and need to comply with the CCPA; or
    c. The company derives more than 50% of its revenues from "selling" California consumer personal information. "Selling" is defined quite broadly to mean the disclosing or making available for monetary or other valuable consideration the personal information of California residents.
4) Given both the broad definition of "personal information" and the fact that the threshold for having to comply with the CCPA is fairly low, virtually any business with contacts into California will have to expend significant effort over the next year to build compliance systems that will:
    a. Make available designated methods for submitting data access requests, including, at a minimum, a toll-free telephone number;[45]
    b. Provide a clear and conspicuous "Do Not Sell My Personal Information" link on the business' Internet homepage, that will direct users to a web page enabling them to opt out of the sale of the resident's personal information;[46]
    c. Implement new systems and processes to verify the identity and authorization of persons who make requests for data access, deletion or portability;
    d. Respond to requests for data access, deletion and portability within 45 days.

[42] CCPA § 1798.175.

[43] *Id.* § 1798.194.

[44] *Id.* § 1798.140(o)(1)

[45] *Id.* § 1798.130(a).

[46] *Id.* § 1798.135(a)(1).

e. Update privacy policies with newly required information, including a description of California residents' rights.[47]
f. Determine the age of California residents to avoid charges that the company "willfully disregards the California resident's age" and implement processes to obtain parental or guardian consent for minors under 13 years and the affirmative consent of minors between 13 and 16 years to data sharing for purposes.[48]

5) The CCPA calls for civil sanctions of:
   a. $7,500 per intentional violation;
   b. $2,500 for any uncorrected unintentional violation.[49]
6) The CCPA creates a private right of action, including subjecting companies that experience a data breach to class action statutory damages of between $100 and 4750 per California resident.[50]
7) Finally, because of fundamental difference between the GDPR and the CCPA, companies cannot rely on GDPR compliance as a safe harbor. For example, the GDPR allows companies the option of provide certain free services in exchange for an opt-in agreement to allow the company to monetize the user's personal information. The CCPA, in contrast, provides that companies cannot refuse to provide services if California residents refuse to opt-in to such monetization.[51]

The outcry from critics to the slap-dash nature of the CCPA has been profound,[52] and California legislators are already at work trying to amend the statute to make it less of a legal minefield.[53] If left in its present form, and if Congress doesn't express preempt it with federal legislation, one commentator put it best:

---

[47] *Id.* § 1798.135(a)(2).

[48] *Id.* § 1798.120(d) (a mini-COPPA requirement).

[49] The statute does not make clear whether making the same mistake to multiple users would result in multiple violations, but we can certainly see where an aggressive attorney general could take the position that, for example, the failure to provide notice of California residents' rights on a webpage would not constitute a single violation, but rather a separate violation for each California visitor.

[50] *Id.* § 1798.150.

[51] *Id.* § 1798.125(a)(1).

[52] *See, e.g.,* Cheryl Miller, *Becerra Rips Lawmakers for 'Unworkable' Provisions in New Data Privacy Law*, The Recorder (Aug. 29, 2018), https://www.law.com/therecorder/2018/08/29/becerra-rips-lawmakers-for-unworkable-provisions-in-new-data-privacy-law/?slreturn=20181009155655.

[53] The California legislature passed SB-1121 in September 2018, intending to correct some of the more glaring errors in the CCPA. *See* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

> Someone will have to pay somehow for the additional compliance efforts required by the California Consumer Privacy Act, including toll-free numbers, privacy notices, opt-in and opt-out mechanisms, data access, data deletion, and data portability, as well as for lost revenue from now prohibited data monetization models and the costs of prosecution, litigation, penalties and statutory damages that businesses will have to pay when they become victims of cyber attacks or data theft even where no one suffers any actual damages. Larger companies may be able to absorb some of the costs or apply expenses to a broader geographic customer base (i.e., consumers in other states or countries). Small businesses in California have far less options. At the end of the day, we as consumers will bear the costs.[54]

IV. The First Amendment

For all the discussion in the U.S. of privacy legislation since the FTC called for its enactment in 2000, there has been precious little discussion of how the First Amendment will affect restrictions upon the flow of information. The FTC's existing consumer protection doctrines developed in large part because of the First Amendment—because the Commission was, until the rise of the Internet, focused overwhelmingly on marketing, which obviously involves the regulation of speech.

The Supreme Court has only begun to grapple with the difficult question of how much of the FTC's regulation of the collection and use of data directly implicates the First Amendment as regulation of speech, rather than conduct. To the extent that it does, any privacy regulation—whether done by the FTC under its existing discussion authority or under new *sui generis* privacy law—will have to be reconciled with the First Amendment, and thus deserve careful consideration in this process. But even to the extent that privacy regulation (and, even more obviously, data security regulation) is not directly subject to the First Amendment, a thoughtful approach to regulation would will begin by studying how the First Amendment has shaped FTC case law thus far, because it illustrates how consumer protection law as evolved under meaningful judicial constraints.

Importantly, the drafters of the GDPR didn't have to deal with the First Amendment at all—creating another reason why U.S. policymakers should not rush to simply copy and paste the GDPR into U.S. law.

[54] Determann, *supra* note 41.

A. The First Amendment & Deception

The FTC's general consumer protection enforcement has avoided most potential First Amendment problems because its primary enforcement tool, at least since 1980, has been deception, affecting, by definition, only speech that is misleading, which the Supreme Court has subjected to only intermediate scrutiny. Even then, the way the FTC has applied its authority illustrates how to regulate complex issues under such scrutiny.

The Court's modern commercial speech jurisprudence began by recognizing the societal value of advertising:

> Advertising, however tasteless and excessive it sometimes may seem, is nonetheless dissemination of information as to who is producing and selling what product, for what reason, and at what price. So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable.

Virginia Bd. of Pharmacy v. *Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748, 765 (1976). The Court rejected what the "State's paternalistic assumption that the public will use truthful, nonmisleading commercial information unwisely," as the Court later summarized its holding in that case, *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 497 (1996):

> There is, of course, an alternative to this highly paternalistic approach. That alternative is to assume that this information is not in itself harmful, that people will perceive their own best interests if only they are well enough informed, and that the best means to that end is to open the channels of communication rather than to close them. If they are truly open, nothing prevents the 'professional' pharmacist from marketing his own assertedly superior product, and contrasting it with that of the low-cost, high-volume prescription drug retailer. But the choice among these alternative approaches is not ours to make or the Virginia General Assembly's. It is precisely this kind of choice, between the dangers of suppressing information, and the dangers of its misuse if it is freely available, that the First Amendment makes for us.

425 U.S. at 770. Building on *Virginia Board*, the Court five years later crafted the level of intermediate scrutiny that applies to this day to the FTC's use of its deception authority:

> The First Amendment's concern for commercial speech is based on the informational function of advertising. See *First National Bank of Boston* v. *Bellotti*, 435 U.S. 765, 783 (1978). Consequently, there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public

> about lawful activity. The government may ban forms of communication more likely to deceive the public than to inform it, *Friedman* v. *Rogers, supra*, at 13, 15-16; *Ohralik* v. *Ohio State Bar Assn., supra*, at 464-465, or commercial speech related to illegal activity, *Pittsburgh Press Co*. v. *Human Relations Comm'n*, 413 U.S. 376, 388 (1973).

Central Hudson Gas Elec. v. Public Serv. Comm'n, 447 U.S. 557, 563-64 (1980). By contrast, non-deceptive "commercial" speech remains subject to strict scrutiny:

> if the communication is neither misleading nor related to unlawful activity, the government's power is more circumscribed. The State must assert a substantial interest to be achieved by restrictions on commercial speech. Moreover, the regulatory technique must be in proportion to that interest. The limitation on expression must be designed carefully to achieve the State's goal. Compliance with this requirement may be measured by two criteria. First, the restriction must directly advance the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government's purpose. Second, if the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.

Id. at 564. While the FTC Act itself defines "false advertisement" as one that is "misleading in a material respect," 15 U.S.C. § 55(a)(1), the Commission's 1983 Deception Policy Statement drew upon *Central Hudson* for one crucial point—that the Commission may presume materiality for explicit claims made in advertisements:

> In the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising.[55]

This sentence has provided the constitutional basis for the vast majority of the Commission's consumer protection work since 1983.

B. The First Amendment & Unfairness

When the Commission applies its unfairness authority to non-misleading speech rather than its deception authority — or, indeed, when Congress attempts to regulates non-misleading speech — it must therefore satisfy strict scrutiny, as explained above: "the asserted governmental interest in the speech restriction must be substantial; the restriction must directly

[55] Fed. Trade Comm'n, FTC Policy Statement on Deception, note 49 (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (hereinafter *Deception Policy Statement*).

advance the governmental interest asserted; and the restriction must not be more extensive than necessary to serve that interest."[56] As then-FTC Commissioner Roscoe Stark explained in a 1997 speech:

> Restrictions on unfair advertising also are subject to First Amendment scrutiny under the *Central Hudson* standard. In *44 Liquormart*, a plurality opinion written by Justice Stevens confirmed that, in the absence of evidence, courts cannot assume that an advertising restraint will significantly reduce consumption. Instead, the government must establish a causal relationship between its speech restriction and the asserted state interest that the restriction is intended to directly advance. The Court found that its earlier decision in *Posadas* — a case that involved a ban on advertising casino gambling — gave too much deference to the legislature when assessing whether a speech restriction directly advances the asserted governmental interest.
>
> In *44 Liquormart*, the Court struck down under the First Amendment a legislative ban on price advertising of alcoholic beverages. The Stevens plurality reasoned that the ban did not significantly advance the asserted governmental interest and was not narrowly tailored. Both the plurality opinion and Justice O'Connor's concurring opinion in *44 Liquormart* agreed that a total ban on price advertising of alcohol — when there were other effective ways for government to achieve its goal — failed to satisfy the *Central Hudson* requirement that a speech restriction not be more extensive than necessary.[57]

Unsurprisingly, the Unfairness Policy Statement, written less than six months after *Central Hudson*, does not discuss the case, whose importance became clear only in the following years. But the three-prong test established by the Policy Statement effectively implements something like the test of strict scrutiny:

1. Establishing **substantial injury** obviously establishes a substantial government interest, provided that they are not "trivial or merely speculative," but noting that "an injury may be sufficiently substantial …. if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[58] This focus on concrete risk, and the associated emphasis on establishing a causal link between the conduct and

[56] Roscoe B. Starek, III, Former Commissioner, FTC, Speech at the American Bar Association Section of Administrative Law and Regulatory Practice Committee on Beverage Alcohol Practice (Aug. 4, 1997).

[57] *Id*.

[58] Fed. Trade Comm'n, FTC Policy Statement on Unfairness, note 12 (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (hereinafter *1980 Unfairness Policy Statement*).

the remedy[59] (the defect identified by the Court in *44 Liquormart*) helps to establish both the substantiality of the government's interest and also the second prong of strict scrutiny, that the regulation must directly advance the governmental interest asserted.

2. The UPS's requirement that the Commission weigh that harm against **countervailing benefits**, broadly understood, addresses both the second and third prongs of strict scrutiny: that the restriction must directly advance the governmental interest asserted and that the restriction must not be more extensive than necessary to serve that interest.
3. Whether consumers themselves **can reasonably avoid** the harm speaks to both the first and third prongs of strict scrutiny: a harm consumers can reasonably avoid is likely not a substantial injury, and the remedy of restricting that speech is also necessarily broader than necessary, since some form of user empowerment would be a less restrictive means of advancing the government's interest.

C. The First Amendment and Privacy Regulation

In short, the Commission's unfairness and deception standards have allowed the Commission to act aggressively to protect consumers while avoiding First Amendment problems in what has been the Commission's historic function: policing marketing. If nothing else, this provides a useful conceptual framework for law makers in thinking about how to craft *any* more specific authority for the Commission.

In privacy regulation, however, the threshold question for the relevance of the First Amendment is when it is speech or conduct that is being regulated. The Court is still in the early stages of working through this question — just as, in the mid-1970s, the Court was still working through whether the First Amendment applied to advertisements at all. But Justice Kennedy's majority opinion in *Sorrell v. IMS Health*, 564 U.S. 552 (2011), suggests the Court will be careful to draw the line in a way that does not entirely exclude data flows from the protection of the First Amendment. The court struck down a Vermont law requiring doctors to opt-in to the use of information by drug companies about the kinds of drugs they prescribe if that information identified them (which it inevitably would, if it were to help drug companies decide how to market drugs to them); on the crucial conduct/speech question, Justice Kennedy wrote:

> This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment. *See, e.g.,* [*Bartnicki v. Vopper*, 532 U.S.

[59] Causation and risk are sometimes broken out as a separate, fourth requirement of the Unfairness Policy Statement and of Section 5(n).

> 514, 527] ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct" (some internal quotation marks omitted)); *Rubin v. Coors Brewing Co.*, 514 U. S. 476, 481 (1995) ("information on beer labels" is speech); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U. S. 749, 759 (1985) (plurality opinion) (credit report is "speech"). ***Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.***[60]

This view is consistent with other Court decisions. In 1971, the Court protected "raw facts" as speech in the so-called "Pentagon Papers case." *N.Y. Times Co. v. United States*, 403 U.S. 713, 714-15 (1971) (Black, J., concurring). The D.C. Circuit recognized that credit reports are speech (but, applying intermediate scrutiny, upheld the restriction) in a challenge brought by a credit reporting agency to the constitutionality of the Fair Credit Reporting Act (FCRA), which forbade companies from sharing consumer credit reports except for specified purposes.[61] The Tenth Circuit concluded that a phone company's using data generated about its consumers in the process of providing them telephone service for marketing to them implicated the First Amendment, and therefore struck down an opt-in requirement as unduly restrictive.[62]

It is still too early to say where the Court will draw lines as to when data practices involve speech and thus when the First Amendment applies to privacy regulations, but the potential applicability of the First Amendment must be a part of any discussion of how new legislation should be crafted. Some potential regulations, such as data breach notification requirements, clearly do implicate speech, yet will likely be easy to justify, because speech may be compelled if it is truthful and objective, and requiring timely notification to consumers that data about them has been compromised seems like an easy case. Some regulations seem relatively clearly focused on conduct—like how well data is secured against loss or theft. But other regulations, like the level of consent required, the ability of users to change or delete information, and, especially, requirements that useful data be destroyed or rendered less useful (through data minimization or required de-identification) seem to implicate the kind of concerns at issue in *Sorrell*. For inclusion in the record, we attach hereto UCLA Law Professor Eugene Volokh's 1999 aptly-titled law review article *Freedom of Speech, Information Privacy,*

---

[60] *Sorrell v. IMS Health*, 564 U.S. 552, 15 (2011).

[61] *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), cert. denied, 536 U.S. 915.

[62] *U.S. West, Inc. v FCC*, 182 F.3d 1224, 1232, 1239-40 (10th Cir. 1999).

and the Troubling Implications of a Right to Stop People from Speaking About You, which predates *Sorrell* but explores some of these questions.[63]

Recognizing the applicability of the First Amendment to the use of personal information does not necessarily mean less regulation, but should mean better and more constitutionally defensible regulation—if only because it will demand a more thoughtful process in drafting legislation and implementing it through regulation or case-by-case enforcement.

Indeed, even those who think the government should have a lower burden in regulating data than it would in regulating speech more generally should find the general approach of First Amendment analysis a useful heuristic for thinking about how best to deal with data: What, exactly, is the government's interest? How substantial is it? Are the means chosen appropriately or narrowly tailored to address that interest? Are they over-broad? Are there other, less restrictive means available to address the problem? Is the approach either over or under-inclusive?[64] These are the questions that have guided the FTC in its development of consumer protection law since 1980. They should continue to guide policymakers in thinking about privacy regulation.

V. An Administrative Law Framework for Privacy

Just as the First Amendment must shape the discussion about privacy law, so must a proper understanding of administrative law. American tech companies have led the world in developing the services so easily taken for granted around the world in no small part because the American approach to privacy has allowed innovative and unexpected uses of data to improve services offered to consumers. Perhaps most critical of all is that entrepreneurs can focus on scaling up new services rather than replicating the elaborate regulatory compliance structures of the incumbent companies whose dominance they are trying to disrupt.

In this sense, two aspects of American privacy law are important and should not be changed lightly. First, we generally rely on the standards of unfairness (with its focus on consumer injury) and deception (with its focus on ensuring that consumers are not misled, either actively or by omission or concealment), with more specific rules limited to areas where consumer injury has been identified by Congress as sufficiently clear to merit more specific rules. Second, tech companies—especially startups—will inevitably make mistakes, or

[63] Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 2 (1999).

[64] *See generally* Berin Szóka, The Progress & Freedom Foundation, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments to the FTC Privacy Roundtables (Dec. 7, 2009), *available at* http://www.scribd.com/doc/22384078/PFF-Comments-on-FTC-Privacy-Workshop-12-7-09.

simply failing to predict where the regulator would decide to draw a line on what is "reasonable"—especially when they are doing things that have never been done quite the same way before. Under the current environment, their legal liability for such mistakes is limited because the FTC cannot impose monetary penalties for first-time violations of Section 5. This section explores both dynamics, the importance of the FTC's burden of proof and the deference it receives, as well as the crucial constitutional requirement that regulated parties receive fair notice of what the law requires.

A. An Evolutionary Approach to Law

The debate over privacy and data security legislation inevitably turns on the advantages and disadvantages of rules versus standards, and whether rules should be fixed in statute, by the regulator, or by courts in crafting their decisions. In a dynamist approach to privacy regulation, both play a role, but the default should be in favor of standards, with rules carefully crafted for narrow circumstances.

"The life of the law," wrote Oliver Wendell Holmes, "has not been logic; it has been experience... The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics."[65] One could say the same for American privacy law — and for American consumer protection law more generally. Europe's GDPR very much resembles the "axioms and corollaries of a book of mathematics," all deduced from the initial, dubious premise that each of us owns all information pertaining to us. The American approach to privacy, by contrast, has evolved over time through something more like the common law method Holmes was describing — on two levels.

First, Congress delegated to the FTC broad consumer protection power under extremely brief statutory standards for unfairness and deception, leaving it to the agency and the courts to better define what those statutes mean over time. Generally, that definition has happened through case-by-case enforcement, except for the brief period in the late 1970s, when the FTC aggressively used the rulemaking powers Congress gave it in 1975.[66] As the FTC's 1980 Unfairness Policy Statement summarized the process:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Con-

[65] Oliver Wendell Holmes, Jr., THE COMMON LAW 1 (1881).

[66] *See generally* J. Howard Beales, Former Director, Bureau of Consumer Protection, Speech at The Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003).

> gress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion.[5] The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[67]

Second, informed by the FTC's experience with its own standards, Congress intervened in several areas to codify certain aspects of the FTC's Section 5 approach with legislation codifying rules or alternative, special-purpose standards, but only in narrow circumstances and after the FTC had attempted to deal with the issue experience.

On the whole, we believe this process of discovery is the best way to approach problems of consumer protection, and that experience suggests that Congress should focus on clearly identified problems, rather than attempting to legislate "comprehensively."

B. Rules v. Standards

The experience of how American consumer protection law developed also suggests a general preference for standards over rules — whether those rules be regulations issued through notice and comment rulemakings, or rules in the broader sense, which can be the output of case-by-case enforcement of a statute. Law Professor Derek Bambauer takes a heterodox view, rejecting the "prevailing consensus in favor of standards for regulating technology," and arguing that "sometimes geeks require rules, not standards."[68] But even he clearly acknowledges that rules work only in limited circumstances:

> instead of seeking to prevent crashes, policymakers should concentrate on enabling us to walk away from them. The focus should be on airbags, not anti-lock brakes. Regulation should seek to allow data to "degrade gracefully," mitigating the harm that occurs when a breach (inevitably) happens.
>
> Such regulatory methods are optimally framed as rules under three conditions. First, **minimal compliance—meeting only the letter of the law—is sufficient to avoid most harm**. Second, **rules should be relatively impervious to decay**

[67] *1980 Unfairness Policy Statement*, *supra* note 58.

[68] Derek Bambauer, 50 Brook. J. Corp. Fin. & Com. L. 49, 50 (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1792824

.

> **in efficacy over time**; technological change, such as increased CPU speeds, should not immediately undermine a rule's preventive impact. Furthermore, **compliance with a rule should be easy and inexpensive to evaluate.** In addition, **rules are likely to be helpful where error costs from standards are high**; where if an entity's judgment about data security is wrong, there is significant risk of harm or risk of significant harm. Finally, this argument has implications for how compliance should be assessed. When regulation is clear and low-cost, it creates an excellent case for a per se negligence rule, or, in other words, a regime of strict liability for failure to comply with the rule.[69]

These circumstances roughly correspond to the areas in which Congress has crafted a rule for specific consumer protection issues in legislation to be enforced alongside Section 5.[70] To these four criteria (not three, as the court stated), we would add a fifth: rules make sense where it is possible to predict, in advance, that the trade-offs involved in a particular issue are so clear-cut that it is possible to decide in advance what the right balance is, and to fix a rule that will decide that issue in a future that is as yet unknown. Judges, in applying the antitrust laws, have faced the same question, deciding when to apply the general rule of reason or to craft a specific per se rule to specific conduct:

> The ultimate question about whether to apply the per se rule depends on whether the challenged practice has characteristics suggesting a more elaborate inquiry under the rule of reason will be either unnecessary or counterproductive.[71]

In theory, the FTC and other regulators play the same role as judges, and so would be equivalent in deciding when to set bright-line rules through case-by-case enforcement. Reality has turned out quite differently, as former FTC Commissioner Josh Wright has lamented:

> Perhaps the most obvious evidence of abuse of process is the fact that over the past two decades, the Commission has almost exclusively ruled in favor of FTC staff. That is, when the ALJ agrees with FTC staff in their role as Complaint Counsel, the Commission affirms liability essentially without fail; when the administrative law judge dares to disagree with FTC staff, the Commission almost universally reverses and finds liability. Justice Potter Stewart's observation that the only consistency in Section 7 of the Clayton Act in the 1960s was that "the Government always wins" applies with even greater force to modern FTC administrative adjudication. Occasionally, there are attempts to defend the FTC's perfect win rate in administrative adjudication by attributing the Commission's superior expertise at choosing winning cases. And don't get me wrong – I agree the agency is pretty

[69] *Id*. at 15.

[70] *See supra* note 24 and 27.

[71] Herbert J. Hovenkamp, *The Rule of Reason,* 70 U. Fla. L. Rev. 81, 91 (2018).

> good at picking cases. But a 100% win rate is not pretty good; Michael Jordan was better than pretty good and made about 83.5% of his free throws during his career, and that was with nobody defending him. One hundred percent isn't Michael Jordan good; it is Michael Jordan in the cartoon movie "Space Jam" dunking from half-court good. Besides being a facially implausible defense – the data also show appeals courts reverse Commission decisions at four times the rate of federal district court judges in antitrust cases suggests otherwise. This is difficult to square with the case-selection theory of the FTC's record in administrative adjudication.[72]

In short, there is little reason to think that FTC Commissioners will provide anything like what the Unfairness Policy Statement called the "the gradual process of judicial inclusion and exclusion" in deciding how to apply their authority generally, and in crafting rules in particular enforcement actions.

In theory, Congress may be better able to make thoughtful decisions about how to craft rules but codifying them in statute raises a different problem: ossification. As the Unfairness Policy Statement recognized, "[t]he statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[73] As true as that was in 1934, it is far truer now, given the pace of technological change. Especially in the area of privacy and data security, with industry practices and consumer demands changing on almost a daily basis, one of the great challenges in this discussion will have to be finding the best way to "future proof" the outputs in terms of rules, standards and policies, to ever-changing technologies.

C. Standards as the Basis for Analytical Rigor

Perhaps even more important than the distinction between rules and standards is the question of how standards are written: Some standards constrain the agency's discretion by explaining what it must do to establish liability, while others simply give the agency broad authority to do whatever it likes (*e.g.*, the FCC's "public interest" standard[74]). This difference at its most extreme, is essentially between a court of law and a court of equity. The FTC has

[72] Joshua D. Wright, Commissioner, Fed. Trade Comm'n, Remarks at the Global Antitrust Institute Invitational Moot Court Competition, 16-17 (Feb. 21, 2015) (emphasis added), https://www.ftc.gov/system/files/documents/public_statements/626231/150221judgingantitrust-1.pdf.

[73] *1980 Unfairness Policy Statement*, *supra* note 58.

[74] The Communications Act of 1934, 47 U.S.C. § 151 et seq.

already been down the road of vast, unchecked discretion in interpreting its "unfairness" power, with disastrous consequences. As Howard Beales explains:

> In 1964, in the Cigarette Rule Statement of Basis and Purpose, the Commission set forth a test for determining whether an act or practice is "unfair": 1) whether the practice "offends public policy" - as set forth in "statutes, the common law, or otherwise"; 2) "whether it is immoral, unethical, oppressive, or unscrupulous; 3) whether it causes substantial injury to consumers (or competitors or other businessmen)." Thus, a new theory of legal liability was born. From 1964 to 1972, the Commission — perhaps because of hostile Congressional reaction to the Cigarette Rule — rarely used its unfairness authority. In 1972, however, the Supreme Court, while reversing the Commission in *Sperry & Hutchinson*, cited the Cigarette Rule unfairness criteria with apparent approval for the proposition that the Commission "like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."
>
> Emboldened by the Supreme Court's dicta, the Commission set forth to test the limits of the unfairness doctrine. Unfortunately, the Court gave no guidance to the Commission on how to weigh the three prongs — even suggesting that the test could properly be read disjunctively. In other words, the Commission now claimed the power to sit as a court in equity over acts and practices within its jurisdiction that either offended public policy, or were immoral, etcetera, or caused substantial injury to consumers. Under the Commission's unfairness authority, thus construed, no consideration need be given to the offsetting benefits that a challenged act or practice may have on consumers.
>
> The result was a series of rulemakings relying upon broad, newly found theories of unfairness that often had no empirical basis, could be based entirely upon the individual Commissioner's personal values, and did not have to consider the ultimate costs to consumers of foregoing their ability to choose freely in the marketplace. Predictably, there were many absurd and harmful results. The most problematic proposals relied heavily on "public policy" with little or no consideration of consumer injury.[75]

As Beales explains, the FTC's overreach in this area nearly led to the agency's destruction by Congress.[76] Any formulation of standards for privacy law should be informed by this experience. Specifically, Congress should attempt to build into standards the kind of elements of analysis that the FTC's 1980 Unfairness Policy Statement developed, which were codified by Congress in 1994 in Section 5(n). This will help to ensure that privacy law develops more in

[75] *See Beales, supra* note 66.

[76] *Id*.

the model of antitrust law, with dueling experts ultimately presenting conflicting evidence before a neutral tribunal. This kind of analytical rigor is unlikely to develop without Congress at least beginning the task of defining what the analysis should include. It will be especially important for standards such as what it means for something to be "proportional to risk" or appropriate for context."

D. Deference & Judicial Review

For decades, the Federal Trade Commission has policed U.S. consumer protection without invoking *Chevron* deference—even in the rare instances where the Commission has actually litigated such cases instead of settling them. Notably, we are not aware of any Commissioner invoking *Chevron* even to support their arguments, as one might expect the full Commission do against minority Commissioners dissenting from a particular opinion. The appeals courts clearly believe *Chevron* does not apply to the Commission. *See, e.g., McWane, Inc. v. FTC*, 783 F.3d 814 (11th Cir. 2015)("We review *de novo* the Commission's legal conclusions and the application of the facts to the law.") (citing *Polypore Int'l, Inc. v. FTC*, 686 F.3d 1208, 1213 (11th Cir. 2012)). Not only does the FTC not get deference on the law, it does not even get deference on the facts: "We also review the application of the facts to the law *de novo.*" *FTC v. Ind. Fed'n of Dentists,* 476 U.S. 447, 454, 106 S.Ct. 2009, 2016, 90 L.Ed.2d 445 (1986).

Prof. Gus Hurwitz has argued that the FTC *could* claim *Chevron* deference—that both the FTC and the courts are mistaken in believing that *Ind. Fed'n of Dentists*, rather than *Chevron* is controlling.[77] This may well be correct as a legal matter, but it is largely irrelevant in that this view would represent a massive shift in how the FTC operates. The *status quo* of American law is that the FTC has developed consumer protection law as well as antitrust law across the board quite well without the need for deference on questions of law (or the application of law to facts). Instead, the FTC has gotten only deference only on questions more clearly limited to factual analysis:

> However, "we afford the FTC some deference as to its informed judgment that a particular commercial practice violates the Federal Trade Commission Act." *Schering-Plough* [*v. FTC]*, 402 F.3d [1056,] 1063 [(11th Cir. 2005)]; *see FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 454 (1986) ("[T]he identification of governing legal standards and their application to the facts found . . . are . . . for the courts to resolve, although even in considering such issues the courts are to give some deference to the Commission's informed judgment that a particular commercial practice is to be condemned as 'unfair' [under the Federal Trade Commission Act].")

[77] Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Common Law*, 101 Iowa L. Rev. 955 (2016).

McWane, 783 F.3d 825.

The single most important issue in drafting any new privacy law, from our perspective, is to preserve the *de facto status quo* of American consumer protection law — so that it will ultimately be courts that determine what the inevitably vague language of statutory standards like "reasonable," "context" and "risk" means. In principle, this is how American consumer protection law was intended to operate. The FTC's 1980 Unfairness Policy Statement makes the point best:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.[78]

Courts, not the FTC, were supposed to decide what the law meant. If anything, the FTC has fallen well short of this model: *despite* not making claim to *Chevron* deference, the fact that the FTC has settled nearly all its enforcement actions with consent decrees means the FTC is, in fact, effectively evading the *de novo* judicial review that the courts and even the Commission seem to believe applies. We have written about this problem at great length elsewhere.[79] This is *not* how privacy law should operate in the future, and yet, the FTC's experience with privacy and data security suggests that both issues are so extraordinarily sensitive that companies are far, far less willing to litigate such cases than, say, antitrust cases. Giving the FTC *Chevron* deference would simply compound the problem dramatically. In short, we believe legislation should make explicit what the courts have already said: that the courts, not the FTC, will decide questions of law (and facts applied to law).

In general, past legislative proposals seem to have avoided this question, both by saying nothing specific on the question of deference and also by incorporating the new legislation

[78] *1980 Unfairness Policy Statement*, *supra* note 58.

[79] *See 2017 FTC Testimony*, *supra* note 1; *2016 FTC Reform Report*, *supra* note 1.

into Section 5. For example, the DATA Act (an earlier version of which was passed by the Democratic-controlled House in 2009[80]) provided that:

> (1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.
>
> (2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.[81]

In effect, this would incorporate the status quo. By contrast, the 2015 Obama legislation specifically requires Courts to "accord substantial weight to the Commission's interpretations as to the legal requirements of [the] Act."[82] As we discuss below, this appears to have been a drafting error, as this provision was placed in the section governing enforcement actions brought by state attorneys general, rather than the FTC itself, and thus appears to have been intended as a limitation upon state AGs' ability to re-interpret the law over the interpretations of the FTC itself — *not* as a shield for the FTC to use against private defendants.

E. Burdens of Proof

What Herb Hovenkamp said of antitrust law would be no less true for any privacy law:

> Of all the procedural issues involved in antitrust litigation under the rule of reason, none are more critical than questions about assignment of the burden of proof and production, and the quality of the evidence that must be presented at each stage.[83]

Under Section 5, the FTC ultimately bears the burden of proof at trial — as well it should. But the ease with which the FTC has managed to settle essentially all of its deception cases, resulting in a so-called "common law of consent decrees" that are "devoid of doctrinal analysis

---

[80] H.R. 2221 - Data Accountability and Trust Act, 111th Congress (2009-2010), https://www.congress.gov/bill/111th-congress/house-bill/2221.

[81] H.R.580 - Data Accountability and Trust Act, 114th Congress (2015-2016), https://www.congress.gov/bill/114th-congress/house-bill/580/text

[82] *2015 CPBR Legislation*, *supra* note 3.

[83] Hovenkamp, *supra* note 54, at 101.

and offer little more than an infinite regress of unadjudicated assertions."[84] Given this problem, we have called on Congress to codify what several courts have already concluded: that the FTC's deception enforcement actions must satisfy the heightened pleading standards of Rule 9(b) of the Federal Rules of Civil Procedure, which applies to claims filed in federal court that "sound in fraud."[85] This requirement would not be difficult for the FTC to meet, since the agency has broad Civil Investigative powers that are not available to normal plaintiffs before filing a complaint.[86] There is no reason the FTC should not have to plead its deception claims with specificity.

The Eleventh Circuit's decision in favor of *LabMD*, discussed below,[87] appears to require specificity akin to that required by Rule 9(b):

> Aside from the installation of LimeWire on a company computer, the complaint alleges no specific unfair acts or practices engaged in by LabMD. Rather, it was LabMD's multiple, unspecified failures to act in creating and operating its data-security program that amounted to an unfair act or practice. Given the breadth of these failures, the Commission attached to its complaint a proposed order which would regulate all aspects of LabMD's datasecurity program—sweeping prophylactic measures to collectively reduce the possibility of employees installing unauthorized programs on their computers and thus exposing consumer information. The proposed cease and desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction.[88]

The same can be said for unfairness claims, even though they do not "sound in fraud." In both cases, getting the FTC to file more particularized complaints is critical, given that the FTC's complaint is, in essentially all cases, the FTC's last word on the matter, supplemented by little more than a press release, and an aid for public comment.

---

[84] *See* Brief of Amici Curiae TechFreedom, International Center for Law and Economics, & Consumer Protection Scholars in Support of Defendants, *FTC. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887), 2013 WL 3739729, *available at* http://techfreedom.org/wp-content/uploads/2018/11/Wyndham-Amici-Brief-TechFreedom-and-ICLE.pdf

[85] *Rombach v. Chang*, 355 F.3d 164, 170 (2d Cir. 2004) ("In deciding this issue, several circuits have distinguished between allegations of fraud and allegations of negligence, applying Rule 9(b) only to claims pleaded under Section 11 and Section 12(a)(2) that sound in fraud.").

[86] *See 2018 TechFreedom FTC Comments,* supra note 1, at 19-22.

[87] *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

[88] *Id.* at 1294-95.

Indeed, the bar should likely be *higher*, not lower for unfairness cases. Former Commissioner Josh Wright has recommended a preponderance of objective standard for unfairness cases.[89] The critical thing to note is that there is no statutory standard for *settling* FTC enforcement actions — so the standard by which the FTC really operates is the very low bar set by Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[90] In addition to the substantive clarifications to the FTC's substantive standards, Congress must clarify either the settlement standard or the pleading standard, if not both.

There is good reason to suspect that the same dynamics may apply in privacy cases, given that it appears that companies' reluctance to litigate privacy cases stems from the extraordinary sensitivity of consumers to headlines about a company's negative track record on privacy. Thus, it may make sense to require pleading with particularity when the FTC brings cases based on standards that are written at a level of conceptual abstraction equivalent to that of Section 5 — such as whether a company's treatment of data, *etc*., is proportional to the risk associated with it (roughly equivalent to unfairness) or appropriate for the "context" of the consumer's interaction with the company, as discussed below.[91] But for more specific rules, the specificity inherent in the rule should suffice to make the FTC's burden clear.

In some instances, providing in statute for shifting burdens of proof may be the best way to build flexibility into a privacy law. For example, whatever the FTC's (or AG's) initial pleading burden might be, if it can show that a company failed to satisfy a particular rule or standard, the burden could shift back to that company. The company could then shift the burden back to the plaintiff by showing that it had, for example, met an industry code of conduct (perhaps one that had been certified by the FTC, as the 2015 Obama privacy legislation proposed), or taken other specific measures, like meeting minimum standards of data de-identification.

F. Fair Notice

Perhaps even more than the First Amendment, the constitutional principle that will shape privacy regulation more than any other is that of Fair Notice. As summarized by FTC practitioner Gerry Stegmaier:

---

[89] Joshua D. Wright, *Revisiting Antitrust Institutions: The Case for Guidelines to Recalibrate the Federal Trade Commission's Section 5 Unfair Methods of Competition Authority*, 4 Concurrences: Competition L.J. 1 at 18-21 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/siting-antitrust-institutions-case-guidelines-recalibrate-federal-trade-commissions-section-5-unfair/concurrences-4-2013.pdf.

[90] 15 U.S.C. § 45(b).

[91] *See infra* at 37-40.

> Generally, the fair notice doctrine reflects society's expectations of "fundamental fairness"—that entities should not be punished for failing to comply with a law about which they could not have known. The doctrine restrains law enforcement officials' discretion by requiring the procedural step of clarifying laws before enforcing them. The issue is whether a law "describes the circumstances with sufficient clarity to provide constitutionally adequate warning of the conduct prohibited."1
>
> The fair notice doctrine initially took root in the context of criminal defense, but in 1968, the U.S. Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") acknowledged the applicability of the doctrine in the civil administrative context. The court observed, "where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."18 Otherwise, the court stated tongue in cheek, penalizing a regulated entity for a reasonable interpretation of a law not matching the agency's unclear interpretation would require the entity to exercise "extraordinary intuition" potentially requiring "the aid of a psychic." Indeed, the D.C. Circuit previously described the situation as resembling "Russian Roulette."[92]

We have written extensively on the FTC's failure to provide fair notice of what Section 5 requires in the area of data security and privacy.[93] Rulemaking is obviously one way to provide fair notice, the value of clear guidance certainly does suggest that, in certain areas, rulemaking could actually be beneficial to regulated parties. For example, much of what the FTC cites as reasonable data security practices seem not to vary at all from case to cases; if these really are so well-established, there may be value in saying so in a rule. But as noted above, rules are not appropriate for every circumstance; many of the principles set forth by NTIA can only be implemented by standards, such as proportionality to risk and respect for context.

In these instances, legislation should give careful thought to how to require the FTC to make full use of the potential toolkit available to it to provide notice of what the law requires — which we have called the "Doctrinal Pyramid"[94] — including:

- Closing letters, explaining why the FTC decided not to take action in a particular investigation, which need not identify the target but could generally describe the fact pattern;

---

[92] Gerard Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 Geo. Mason L. Rev., No. 3, 673 (2013).

[93] *See, e.g.*, *TechFreedom 2018 Testimony*, *supra* note 1, at 31-35; 2016 FTC Reform Report, supra note 1, at 38-42.

[94] *TechFreedom 2018 Testimony*, *supra* note 1, at 12-13.

- No-action letters, explaining why the FTC would not take action in a fact pattern submitted to it by a company seeking guidance;
- Policy statements on specific issues;
- Industry guides, such as the Green Guides; and
- Reports based on workshops.

We have given particular attention to the Green Guides as a model for how the FTC can summarize its past enforcement actions in a way that provides meaningful fair notice.[95] But as we have noted, the most important form of guidance comes from actually litigated cased, resulting in decisions on the merits by a federal judge. In this sense, our concerns about the dynamics of enforcement skewing wildly in favor of the agency and thus causing companies to settle privacy and data security enforcement actions, discussed below,[96] are as much concerns about a systemic failure to provide the most meaningful form of fair notice to all potentially affected parties as they are concerns about a lack of procedural fairness to specific defendants.

G. Civil Penalties

Another key aspect of the ongoing debate over privacy legislation has been under what circumstances the FTC will be able to impose civil penalties. Congress has specifically authorized the FTC to seek civil penalties for violations of certain statutes, e.g., the CAN–SPAM Act, 15 U.S.C. § 7701 et seq. But in general, the FTC cannot impose civil penalties for first-time violations of Section 5. We believe there is a place for civil penalties, just as there is for rules, but that both should be limited to specific, narrow circumstances. Indeed, the two should generally coincide, because civil penalties should be imposed only where a regulated party has been provided fair notice of what the law requires.

Even under Democratic leadership, the FTC has been careful to argue for a focused application of civil penalty authority. In 2016 Congressional testimony, for example, the FTC said: "To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations ***in appropriate circumstances***."[97] The testimony did not specify what would constitute "appropriate circumstances." In Congressional testimony earlier this year, the Commission said something similarly vague:

---

[95] *Id.* at 31-46.

[96] *See infra* at 33

[97] Prepared Statement of the Federal Trade Commission: Opportunities and Challenges in Advancing Health Information Technology, House Oversight and Government reform Subcommittees on Information technology and Health, Benefits and Administrative Rules, Washington, D.C. (March 22, 2016) at 7, https://oversight.house.gov/wp-content/uploads/2016/03/2016-03-22-Rich-Testimony-FTC.pdf

> Section 5, however, cannot address all privacy and data security concerns in the marketplace. For example, ***Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability***. The Commission also lacks authority over non-profits and over common carrier activity, even though these acts or practices often have serious implications for consumer privacy and data security. Finally, the FTC lacks broad APA rulemaking authority for privacy and data security generally. The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation.[98]

Likewise, the FTC took a similarly narrow position in favor of civil penalties in 2008, in testimony before the Senate Commerce Committee held on an FTC reauthorization bill that would have given the FTC broad civil penalty authority. The FTC's prepared statement, approved by all five Commissioners, said:

> As the Commission has previously testified, however, in certain ***categories of cases restitution or disgorgement may not be appropriate or sufficient remedies***. These categories of cases, where civil penalties could enable the Commission to better achieve the law enforcement goal of deterrence, include malware (spyware), data security, and telephone records pretexting. In these cases, consumers have not simply bought a product or service from the defendants following defendant's misrepresentations, and it is often difficult to calculate consumer losses or connect those losses to the violation for the purpose of determining a restitution amount. Disgorgement may also be problematic. In data security cases, defendants may not have actually profited from their unlawful acts. For example, in a case arising from a data security breach enabled by lax storage methods, the entity responsible for the weak security may not have profited from its failure to protect the information; rather, the identity thief who stole the information likely profited. In pretexting and spyware cases, the Commission has found that defendants' profits are often slim; thus, disgorgement may be an inadequate deterrent. Also in pretexting and spyware cases, lawful acts and unlawful acts may be intermixed; thus, it may be difficult to determine an appropriate disgorgement amount. And in a whole host of cases brought under Section 5, when we are challenging hard-core fraud that could otherwise be prosecuted criminally, we should be able to seek fines against these wrongdoers.[99]

---

[98] Prepared Statement of the Federal Trade Commission, "Oversight of the Federal Trade Commission," before House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection, Washington, D.C. at 6 (July 18, 2016), https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

[99] *Hearing on Fed. Trade Commission Reauthorization, before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. 2 at 17 (2008), https://www.gpo.gov/fdsys/pkg/CHRG-110shrg75166/pdf/CHRG-110shrg75166.pdf.

By contrast, the Obama Administration's proposed 2015 legislation would have given the FTC the ability to impose civil penalty authority for *any* violation of the law — with even higher penalties "[i]f the Commission provides notice to a covered entity, stated with particularity, that identifies a violation of this Act."[100]

Giving the FTC civil penalty authority across the board — whether across Section 5 or across a law spanning a subject area as vast as "privacy" — risks three problems.

1. Companies may be penalized without fair notice. Whether or not the agency is able to meet the constitutional standard for fair notice as interpreted thus far by the courts, the problem of fairness to regulated parties will remain.
2. Second, just as civil penalties can be valuable for deterrence in areas where companies might fail to take a particular concern seriously enough (*e.g.,* by underinvesting in cybersecurity), the *in terrorem* effect of civil penalties can create a strong incentive for companies to be overly cautious in deciding where to fall in a spectrum of potential compliance options. In particular, they may become overly cautious about developing new products. It is for this reason that civil penalties should be reserved for cases of clear harm to consumers, rather than cases where a company may simply strike a balance that the FTC later decides was not the right one.
3. The threat of imposing civil penalties greatly increases the leverage regulators have over the companies they regulate. This makes it easier both to persuade companies to settle and also to use settlements to extract other concessions from the company.

VI. Enforcement

The RFC asks:

> One of the high-level end-state goals is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority? [100]

Before we define the proper role and enforcement tools the FTC should use, we must first explore the question of how privacy protection fits into America's overall federal system of laws. We must also examine whether private rights of action are an effective and appropriate tool.

---

[100] *2015 CPBR Legislation*, *supra* note 3.

[100] *RFC, supra* note 6, at 48603.

A. Federalism & Preemption

The Internet is an inherently interstate medium, and states must be preempted from layering on privacy and data security regulations that conflict with federal policies. We have written extensively on why state regulation of the Internet must be preempted.[101] Therefore, any federal legislation should contain explicit preemption of state regulation of consumer privacy, lest states argue that the have a right to impose additional regulations in order to protect consumers in their states.

The proper role for state attorneys general is to enforce their own Baby FTC Acts, as well as issue-specific pieces of legislation such as COPPA and the CAN-SPAM Act.[102] They can and should supplement enforcement of any more specific privacy legislation. This will bring both additional resources to bear on privacy problems, and also ensure that appropriate attention is paid to privacy violations throughout the country that might not attract the attention of the FTC if the Commission had sole authority for enforcing its laws.

But by the same token, we must be realistic about two downsides of enforcement by state AGs: (1) overly politicized enforcement and (2) doctrinal divergence. Today, 43 states directly elect their Attorney General. This makes the vast majority of AGs inherently political; and even those that are not elected are far more political than the typical FTC Commissioner, if only because their appointment is often a stepping stone to the governor's mansion, or to running for the House or Senate. By contrast, the FTC was carefully designed to be immune from political pressure. State AGs have obvious incentives to bring high-profile cases against high-profile Internet companies to make headlines and pad their political resumes. Such weaponization of privacy law is a problem in itself, but it also risks exacerbating a second problem: that the interpretation of the law could fracture significantly, with states, rather than the FTC, shaping doctrine, especially as to the meaning of inherently vague standards.

The legislation proposed by President Obama in 2015 included three safeguards to address both problems:

1. Unless the FTC joined a state's enforcement action, the state AG would be limited to obtaining injunctive relief.[103]
2. The bill required courts reviewing AG enforcement actions to "accord substantial weight to the Commission's interpretations as to the legal requirements of [the] Act" — making it difficult for state AGs to change the course of doctrine on their own.

---

[101] *See* Owens, *supra* note 40.

[102] *See* 15 U.S.C. § 7706(f) (state attorneys general may bring a civil action in federal court on behalf of citizens of the state).

[103] *2015 CPBR Legislation*, *supra* note 3, § 202(a).

3. Finally, the bill required state AGs to notify the FTC at least 30 days prior to bringing such enforcement actions. While the FTC would not have had the legal right to stop such suits, prior notification at least gave the FTC the opportunity to privately dissuade AGs from bringing legally shaky or opportunistic suits and, if necessary, to comment publicly upon such suits once filed.

We believe all three safeguards are essential, but may not be adequate to guard against abuse. In particular, our study of how the FTC has built its so-called "common law of consent decrees" suggests that the Commission's enormous leverage in its own investigative process is essential to the Commission's ability to coerce companies into settling legally questionable cases.[104] We have made several suggestions geared towards re-balancing the dynamics between the FTC and the companies it regulates, such as allowing companies the ability to move to quash the FTC's Civil Investigative Demands.[105] We worry that, without federal safeguards on an investigative process, a state AG could use its investigative powers to harass Internet companies.

B. Private Right of Action

Private rights of action as an enforcement tool can be a powerful, and often dangerous, enforcement tool. As noted above, the GDPR creates private rights of action, and it took just a matter of hours before lawsuits were filed claiming GDPR violations and demanding $8.8 billion in damages. Here in the United States, there have been high-profile abuses of the TCPA, which also contains a private right of action.[106] Given the obvious potential for abuse, it is not surprising that President Obama's 2015 Obama Consumer Privacy Bill of Right legislation did not contain a private right of action. This should be the starting place for any discussion of legislation from *both* sides of the aisle.

Including private rights of actions in consumer statutes are the most troubling in the context of class action suits and the use of "cy pres" awards—the practice of distributing class action settlement money to court-approved charities instead of class members, which many allege perverts the intention of the federal rules enabling class actions.[107]

---

[104] *2017 FTC Testimony*, *supra* note 1, at 43.

[105] *Id.* at 21.

[106] *See* TCPA Litigation Sprawl, *supra* note 36.

[107] *See* Alison Frankel, *Should SCOTUS Review Cy Pres-only Settlements?*, Reuters (Mar. 12, 2018), https://www.reuters.com/article/legal-us-otc-cypres/should-scotus-review-cy-pres-only-settlements-google-says-no-need-idUSKCN1GO2IW.

There is also a fundamental question of whether class members must prove actual concrete injury rather than merely alleging a statutory violation under the *Spokeo* standard.[108] In recent oral arguments held on October 31, 2018 in *Frank v. Gaos,*[109] several Supreme Court justices questioned whether they could even reach the fairness question of a *cy pres* settlement when the court below failed to determine whether class members had standing.[110]

Given the unsettled state of the law from a constitutional standpoint, Congress should be circumspect at least, and more likely reluctant, to adopt broad privacy private rights of action in any future privacy legislation. It Congress does enact a privacy private right of action, it must somehow deal with both the issue of the fundamental fairness of *cy pres* settlements, and determine how to deal with the question of standing. As to the latter, it could either attempt to define the types of harm that meet the constitutional standard of being "concrete and particularized," or it could explicitly delegate that task to the FTC to determine standing either through a rulemaking proceeding, or develop such standards through case-by-case adjudications.[111]

VII. Specific Comments on Proposed Principles

A. Principle #0: De-Identification of Personal Information

The most important aspect of any privacy regulatory framework is the scope of covered information. While not specifically addressed in the RFC, this issue will undergird any approach in this area. In comments we filed with NITA in July on the agency's international priorities, we noted that:

[108] *Spokeo, Inc. v. Robins*, 578 U.S. ___ (2016). *Spokeo* involved a class action suit brought under the Fair Credits Reporting Act (FCRA), 15 U.S.C. § 1681, where the lead class member claimed that incorrect personal information about him on the spokeo.com website was an FCRA violation. The Ninth Circuit concluded that Robins had demonstrated sufficient harm for standing, but the Supreme Court reversed, finding that the harm was not "concrete and particularized" as required under Article III of the United States Constitution.

[109] *Frank v. Gaos,* 138 S.Ct. 1697 (2018) (No. 17-961). The case involves the fairness of a class action settlement of $8.5 million by Google and counsel for class members included only the payment of attorney fees and cy pres contributions to several charities, and nothing to class members.

[110] *See* Alison Frankel, *Justices revisit Spokeo standing at oral arguments over cy pres settlements*, Reuters (Nov. 1, 2018) https://www.reuters.com/article/us-otc-cypres/justices-revisit-spokeo-standing-at-oral-arguments-over-cy-pres-settlements-idUSKCN1N660K. As the article notes, however, the lower court in *Frank* approved the settlement prior to the Supreme Court's decision in *Spokeo.*

[111] Whether a case-by-case development of privacy injury standard is possible where private litigants are using statutory private rights of action is questionable.

> while the GDPR recognizes, in principle, that information that can no longer be "attributed to a natural person" no longer requires the protections of the regulations, it sets an exceedingly high bar in satisfying this anonymization standard—and fails to encourage data controllers to bother attempting to deidentify data.[112]

Specifically, the GDPR defines anonymization (literal impossibility of deriving insights on a discreet individual), it does not define pseudonymization:

> Whether pseudonymized data is "reasonably likely" to be re-identified is a question of fact that depends on a number of factors such as the technique used to pseudonymize the data, where the additional identifiable data is stored in relation to the de-identified data, and the likelihood that non-identifiable data elements may be used together to identify an individual. Unfortunately, the Article 29 Working Party has not yet released guidance on pseudonymization and what techniques may be appropriate to use.[113]

As we noted:

> This legal uncertainty, which in turn serves to discourage de-identification of data, perhaps more than any other aspect of GDPR, reflects an elevation of theoretical privacy concerns above practical concerns like cost—even while paying lip service to such concerns. Such an all-or-nothing, strict-liability approach is utterly incompatible with American privacy law— and, indeed, with the overwhelming consensus among privacy scholars that regulating data differently, depending on whether, and how effectively, it has been de-identified, will benefit users both by making possible beneficial uses of identified, aggregate data while also incentivizing companies not to retain data in identified form when they do not need to do so.[114]

The FTC's 2012 Privacy Report takes a reasonable approach:

> First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about,

---

[112] Comments of TechFreedom, In the Matter International Internet Policy Priorities, Docket No. 180124068–8068–01 (July 16, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/comments_of_techfreedom_re_ntia_noi.pdf.

[113] Matt Wes, Looking to Comply With GDPR? Here is a primer on anonymization and pseudonymization, IAPP (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/.

[114] NTIA International Priorities at 8-9.

> or otherwise be linked to, a particular consumer, computer, or other device. Consistent with the Commission's approach in its data security cases, what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant. Thus, for example, whether a company publishes data externally affects whether the steps it has taken to de-identify data are considered reasonable. The standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified.[115]

Just as there should be an incentive to use less identifying, more aggregate information where you can, so, too, should there be an incentive to treat sensitive information — whether based on the risk involved, the context from which it is derived or in which it is used, or its inherent de-identifiability (e.g., biometrics) — with particular attention. Failing to recognize such spectrums will, in essence, mean prioritizing everything, which, in turn, means prioritizing nothing.

Finally, it would be a mistake to rely solely on discouraging the use of identifiable data — what one might call the "abstinence-only approach" to data protection — through regulation. Government also has a valuable role to play in helping to advance the state of the art in deidentification through funding research and the dissemination of best practices across American business.

B. Principle #1: Transparency

Given its generality, the RFC's wording of this principle seems uncontroversial. We would add only one thing. The paragraph defining this principle concludes as follows:

> Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.[116]

---

[115] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 21 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. [hereinafter "2012 Privacy Report"].

[116] *RFC*, *supra* note 6, at 48601.

We suggest making a more specific reference to the concept of Smart Disclosure — the idea that disclosures, in addition to being made in machine-readable form (privacy policies, privacy labels, *etc*.) should also be made disclosures into machine-readable code. This concept was first recognized in 2011 by an official memorandum issued by the Office of Information and Regulatory Affairs (OIRA) to the heads of executive departments and agencies:

> Smart disclosure makes information not merely available, but also accessible and usable, by structuring disclosed data in standardized, machine readable formats. Such data should also be timely, interoperable, and adaptable to market innovation, as well as disclosed in ways that fully protect consumer privacy. In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.[117]

Machine-readable disclosures are the best way to provide consumers with meaningful choice: they enable innovation in how human beings process information, and avoid having to rely upon a single, one-size-fits-all disclosure.

They also empower user agents to act on our behalf: while today's browsers, browser extensions and mobile operating systems may be relatively simply, these tools are becoming increasingly sophisticated. Providing them with standardized, machine-readable information about privacy practices will make it possible for these tools to assist us in making smarter decisions about our privacy.

C. Principle #2: Control

> Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity.[118]

---

[117] Office of Information and Regulatory Affairs, Exec. Office Of The President, Memorandum for the Heads of Executive Departments and Agencies: *Informing Consumers through Smart Disclosure* (Sept. 8, 2011), https://obamawhitehouse.archives.gov/sites/default/files/omb/inforeg/for-agencies/informingconsumers-through-smart-disclosure.pdf.

[118] *RFC*, *supra* note 6, at 48601.

This proposed framing introduces a vital distinction missing from the 2012 Consumer Privacy Bill of Rights, and from past privacy proposals generally. It merits further development.

Users "**provide**" information when, for example, they post status updates, photos, or videos, write emails, documents or Slack messages. It makes sense for a robust control principle to govern such information, for two reasons. First, it is of a kind that users would reasonably expect to be able to control. While we are generally skeptical of the property rights metaphor for personal information, it works best with respect to information that is actively provided by users.

By contrast, much of the information collected online and by digital services and devices is simply ***observed*** about how users act. This information may be sensitive and could even carry the risk of harm to users, but it is not generally the kind of information over which users have an inherent reasonable expectation of control — unless it is associated with risk or otherwise sensitive. Put differently, such information should well be covered by other privacy principles, but that does not mean it ought to be covered by this one. Indeed, attempting to apply a control principle to all such information would simply result in diluting the control principle across the board. Thus, users' privacy may be better served by a more limited, but stronger, control principle.

(There are two additional categories of information: (1) **inferences**, which may be drawn based either on information provided by, or observed about, users and (2) **aggregate information**, which may be distilled from either information provided by, or observed about, users.)

Since the debate about user control is usually distilled into the opt-in v. opt-out debate, and given the oversized importance of the GPDR in this debate, it bears special emphasis that the GDPR is not, contrary to popular assumption, an opt-in only regime. In fact the GDPR recognizes that opt-out is appropriate in multiple contexts and that, in other circumstances, control is simply not appropriate at all. One of the most valuable concepts offered by the GDPR is that of "legitimate interests": effectively, you can't object to all processing if you want the service to work.[119]

Indeed, if the information is truly necessary to the provision of the service, there shouldn't be a right to object at all. As former FTC Chairman Muris has noted, the credit reporting system regulated by FCRA "works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent

[119] Commission Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.

were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse."[120]

For information that is *not* strictly necessary for the provision of a service, some predictive judgment is required: if the use of the information is generally beneficial, opt-out should be the rule. But if the use of that information is high-risk, opt-in should be required.

D. Principle #3: Reasonable Minimization (Context & Risk)

> Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm. Other means of reducing the risk of privacy harm (e.g., additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization.[121]

This framing references, and effectively blends the FTC's long-standing concepts of deception and unfairness—the heart of the FTC's Section 5 consumer protection powers.

1. Risk, Injury & the Lasting Relevance of the "Unfairness" Standard

Most obviously, "risk of privacy harm" is effectively a modified version of the FTC's unfairness doctrine, allowing for the possibility that either the statute or the agency, exercising greater discretion than that allowed by the FTC's 1980 Unfairness Policy Statement, might recognize additional categories of harms that might not be easily cognizable under that policy. The Policy Statement bears quotation in key part here:

> First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers, as has been suggested in some of the comments.[16]

---

[120] Timothy J. Muris, Former Chairman, FTC, Remarks at Privacy 2001 Conference: Protecting Consumers' Privacy: 2002 and Beyond (Oct. 4, 2001).

[121] *RFC*, *supra* note 6, at 48601.

> [16] … In an extreme case, however, where tangible injury could be clearly demonstrated, emotional effects might possibly be considered as the basis for a finding of unfairness. *Cf*. 15 U.S.C. 1692 *et seq.* (Fair Debt Collection Practices Act) (banning, eg., harassing late-night telephone calls).[122]

It would be perfectly appropriate for Congress to define additional categories of injuries — and better for Congress to do so than for the FTC to try to undermine the discipline that the Unfairness Policy Statement has brought to the FTC's interpretation of its uniquely vague "unfairness" authority. To the extent that Congress decides to delegate to the FTC discretion over such categorization, it is essential that the Commission provide fair notice to regulated parties that the kinds of data they are treating may trigger additional legal duties — for all the reasons discussed above.[123]

Furthermore, expanding the definition of harm does not require taking an evaluation of privacy harms out of the analytical framework of unfairness. Indeed, expanding the definition of harm will make it *more*, not less, important that the Commission assess the other two factors set forth in the Unfairness Policy Statement and enshrined in Section 5(n):

> Second, the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces. Most business practices entail a mixture of economic and other costs and benefits for purchasers. A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article. The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.[124]

And finally:

> the injury must be one which consumers could not reasonably have avoided. Normally we expect the marketplace to be self-correcting, and we rely on consumer choice-the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most

[122] *1980 Unfairness Policy Statement*, *supra* note 58.

[123] *Id.*

[124] *Id*.

> desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.[125]

2. Context, User Expectations & the Lasting Relevance of the "Deception" Standard

Similarly, a respect for "context" evokes the same fundamental ideas about consumer sovereignty behind the FTC's bedrock deception authority.[126] The concept of respect for context will inevitably play a key role in any future privacy approach, but it requires limiting principles, lest it be a blank check for regulators, denying companies fair notice of what is required of them. The obvious limiting principle is the same one at the heart of the FTC's deception power: materiality. While the Unfairness Policy Statement makes clear that "[u]njustified consumer injury is the primary focus of the FTC Act,"[127] the Deception Policy Statement does not actually require proof of injury. Instead, materiality — *i.e.*, relevance to the reasonable consumer's decision-making — operates as a proxy for injury:

> the representation, omission, or practice must be a "material" one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception. In many instances, materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary.[128]
>
> ….
>
> A finding of materiality is also a finding that injury is likely to exist because of the representation, omission, sales practice, or marketing technique. Injury to consumers can take many forms. Injury exists if consumers would have chosen differently but for the deception. If different choices are likely, the claim is material,

---

[125] *Id.*

[126] *RFC*, *supra* note 6.

[127] *1980 Unfairness Policy Statement*, *supra* note 58.

[128] *Deception Policy Statement*, *supra* note 55, at 1.

> and injury is likely as well. Thus, injury and materiality are different names for the same concept.[129]

At least a first approximation, the right question to ask about context is whether reasonable consumers would have chosen differently if they had been fully informed about the practice. Or, put differently, whether the context of their interaction with a company collecting data about them made it reasonable for them to expect that the company would act in a certain manner regarding their data.

Unfortunately, while the FTC's nearly two decades of privacy and data security enforcement actions have rested primarily on the agency's deception (rather than its unfairness) authority, few of these cases tell us much about how to analyze materiality, because the FTC has generally bypassed the materiality requirement by simply invoking the Deception Policy Statement's presumption that any express statement is material (on top of the presumption that any failure to live up to a material statement is harmful).[130] Nonetheless, the Commission *has* had to confront these questions in the context of its material *omission* cases, and these cases offer a useful starting place in how to think about materiality.

3. How the Commission Pleads Cases

Given the discussion above, it bears emphasizing here two key advantages to maintaining consistency between any new privacy legislation and the well-established concepts of deception and unfairness: First, in its enforcement actions, the Commission is likely to plead theories under both Section 5 and its new authority. Second, in addition to the Commission's law enforcement function, its workshops, reports, guidance, testimony and advocacy work together play a key role in shaping the policy discussion around some of the most important issues in America. That work should ultimately rest on the Commission's legal authority, which provides a conceptual framework for the Commission's analysis and policy formulation. The more directly the Commission draws upon the bedrock concepts of consumer protection law, the more coherent will be its policy outputs.

E. Principle #4: Security

> Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or

[129] *Id*. at 6.

[130] *Nomi Paper*, *supra* note 1.

> improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available. Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data.[131]

Two concepts require further emphasis here: (1) how cost-benefit analysis applies to data security and (2) how comparison to industry practice will work.

1. Cost-Benefit Analysis.

Any data security framework will ultimately turn on the economic question of how much data security is enough. When the NTIA's principle says "organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data," it is really saying that organizations should have a duty to spend resources on data security that are commensurate with the risks associated with the data. This cost-benefit analysis is implicit in the current standard for unfairness, on which the FTC's data security actions to date have partly rested. Unfortunately, the FTC has grounded most of those actions in, or primarily in, its deception authority, and has, in that context, refused to ground the assessment of "reasonableness" in data security in cost-benefit terms. This has left the Commission's approach to data security fundamentally arbitrary. We have written about this problem at great length in Congressional testimony and reports on the FTC's current shortcomings and the need for reform.[132] Our testimony before the Senate Commerce Committee last year offers a brief synopsis of our views:

> Conversely, despite all of the FTC's rhetoric about "reasonableness" — which, as one might "reasonably" expect, should theoretically resemble a negligence-like framework — the FTC's approach to assessing whether a data security practice is unfair under Section 5 actually more closely resembles a rule of strict liability. Indeed, rather than conduct any analysis showing that (1) the company owed a duty to consumers and (2) how that the company's breach of that duty was the cause of the breach — either directly or proximately— which injured the consumer, instead, as one judge noted, the FTC "kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…."
>
> There is no level of prudence that can avert every foreseeable harm. A crucial underpinning of calculating liability in civil suits is that some accidents are unforeseeable, some damages fall out of the chain of causation, and mitigation does not always equal complete prevention. Thus our civil jurisprudence acknowledges

[131] *RFC*, *supra* note 6, at 48601-2.

[132] *2017 FTC Testimony*, *supra* note 1, at 27; *2016 FTC Reform Report*, *supra* note 1, at 98-99.

> that no amount of care can prevent all accidents (fires, car crashes, etc.), or at least the standard of care required to achieve an accident rate near zero would be wildly disproportionate, paternalistic, and unrealistic to real-world applications (e.g., setting the speed limit at 5 mph).[133]

Any privacy law framework should clearly require an assessment of the costs as well as benefits of data security. Absent such a requirement, the system will be completely one-sided: what basis will any defendant ever have for defending itself?

Importantly, to the extent that legislation expands the definition of harm beyond that which could have been (easily) cognizable under Section 5 generally, that is all the more reason for the assessment of the reasonableness of data security to be grounded clearly in the otherwise-applicable framework of Section 5(n): the potential to cause harm (however defined) that consumers cannot reasonably avoid weighed against countervailing benefit. It would be a mistake to, on top of expanding the definition of harm, build in *additional* discretion for the regulator to decide what is "reasonable."

2. Comparison to Industry Practice.

Our study of the FTC's data security enforcement actions reveals a second serious flaw in the FTC's analysis of "reasonableness": while the FTC has purported to assess one company's data security practices against some kind of "standard practice," in the only fully litigated case in this area, the Commission failed to offer any meaningful comparison. Perhaps the most shocking thing about the *LabMD* litigation was that, after six years of investigating the Georgia small business that ran a cancer testing lab with 30 employees and $4 million in annual sales,[134] the FTC's expert witness could only speak to the data security practices of Fortune 1000 companies.[135]

To some degree, such problems are inherent in attempting to compare one company's practices with those of a comparable class — which suggests that the primary focus of data security enforcement should be on the cost-benefit analysis outlined above. But to the extent that the reasonableness of one company's data security practices is measured against those of

---

[133] *2017 FTC Testimony, supra* note 1, at 29.

[134] Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off: Michael Daugherty learns the high price of resistance*, Bloomberg (Apr. 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/.

[135] Gus Hurwitz, *The FTC's Data Security Error: Treating Small Businesses Like the Fortune 1000* (Feb. 20, 2017), https://www.forbes.com/sites/washingtonbytes/2017/02/20/the-ftcs-data-securityerror-treating-small-businesses-like-the-fortune-1000/#58d2b735a825.

other companies, the FTC should have to clearly define a comparable class of similarly situated companies and compare *their* practices against the defendant's.

This offers one important advantage: it would encourage industries to develop their own best practices, if only to preempt the FTC in defining (a) the class of companies to which they belong and (b) the practices they believe are reasonable. The best way to encourage such efforts is to give them some formal legal standing as safe harbors, as the 2015 Obama legislation would have done.[136]

3. Causation

NTIA's proposed risk principle implies that the Commission would have to establish some kind of causal link between a data practice and consumer injury. How that link must be established is already a subject of litigation that should inform this crucial part of any privacy framework.

Section 5(n) currently requires that:

> The Commission shall have no authority … to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[137]

The words "causes or is likely to cause" were recently the subject of the FTC's litigation against LabMD. In 2015, after an evidentiary hearing, the ALJ dismissed the FTC's complaint, having concluded that the FTC failed to prove that LabMD's "alleged failure to employ reasonable data security . . . caused or is likely to cause substantial injury to consumers."[138] The full Commission reversed later that year — unsurprisingly.[139] But this year, the Eleventh Circuit found for the company, ruling that, while the FTC's unfairness power may be used to bar specific practices, it cannot require a company "to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[140]

---

[136] *2015 CPBR Legislation*, *supra* note 3.

[137] 15 U.S.C. § 45(n).

[138] LabMD, Inc., No. 9357, 2015 WL 7575033, at *48 (MSNET Nov. 13, 2015), https://causeofaction.org/wp-content/uploads/2015/11/Docket-9357-LabMD-Initial-Decison-electronic-version-pursuant-to-FTC-Rule-3-51c21.pdf.

[139] LabMD, Inc., No. 9357, 2016 WL 1446073 https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf. *See supra* note 72 (former FTC Commissioner Josh Wright explaining the FTC's record of *always* finding in its favor on appeal from ALJ decisions finding for defendants).

[140] *LabMD v FTC*, *supra* note 88, at 27.

The court concluded that the FTC *might* have established causation (or at least, made a plausible allegation of causation) in one limited respect:

> the FTC's complaint alleges that LimeWire was installed on the computer used by LabMD's billing manager. This installation was contrary to company policy. The complaint then alleges that LimeWire's installation caused the 1718 File, which consisted of consumers' personal information, to be exposed. The 1718 File's exposure caused consumers injury by infringing upon their right of privacy. Thus, the complaint alleges that LimeWire was installed in defiance of LabMD policy and caused the alleged consumer injury. Had the complaint stopped there, a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers.
>
> But the complaint continues past this single allegation of wrongdoing, adding that LimeWire's installation was not the only conduct that caused the 1718 File to be exposed. It also alleges broadly that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." The complaint then provides a litany of security measures that LabMD failed to employ, each setting out in general terms a deficiency in LabMD's data-security protocol. Because LabMD failed to employ these measures, the Commission's theory goes, LimeWire was able to be installed on the billing manager's computer. LabMD's policy forbidding employees from installing programs like LimeWire was insufficient.
>
> The FTC's complaint, therefore, uses LimeWire's installation, and the 1718 File's exposure, as an entry point to broadly allege that LabMD's data-security operations are deficient as a whole. Aside from the installation of LimeWire on a company computer, the complaint alleges no specific unfair acts or practices engaged in by LabMD. Rather, it was LabMD's multiple, unspecified failures to act in creating and operating its data-security program that amounted to an unfair act or practice. Given the breadth of these failures, the Commission attached to its complaint a proposed order which would regulate all aspects of LabMD's data security program—sweeping prophylactic measures to collectively reduce the possibility of employees installing unauthorized programs on their computers and thus exposing consumer information. The proposed cease and desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction.[141]

[141] *Id*. at 1294.

In short, the court ruled, the Commission had failed to establish the "risk" created by LabMD's practices — other, perhaps, than its failure to enforce its policy against the unauthorized installation of data on company computers by staff. The Commission has yet to grapple with this decision, and it remains to be seen how this case will affect the Commission's approach to data security (or privacy, given that some privacy enforcement actions could rest on the same question of causation under unfairness), as well as how courts in other circuits will rule on this question.

Our *amicus* brief in support of LabMD before the Eleventh Circuit provides a full analysis of how the FTC has, in our view, attempted to effectively rewrite Section 5(n)'s "likely to cause" language to mean, in practice, that the FTC could find unfair a practice that merely creates the *possibility* of harm.

> The fundamental problem with the FTC's argument is that, by arguing backward solely from what eventually did occur, and failing to assess the ex ante risk that it as well as all other possible security problems would occur, the FTC puts the cart before the horse and effectively converts a negligence-like regime into one of strict liability. The duty of care that must be violated for a "reasonableness" standard is meaningless if it is defined solely by such a narrow, post hoc analysis. By effectively defining "reasonableness" in terms of a company's failure to thwart only the breach that did occur (and not the ones that could have but did not), the analysis becomes one of effective strict liability.[142]

The ALJ's decision put it best:

> As the Commission stated in *International Harvester*, to suggest that there is a kind of risk that is separate from statistical risk "amounts really to no more than a conversational use of the term in the sense of 'at risk.'" In this sense everyone is 'at risk' at every moment, with respect to every danger which may possibly occur. When divorced from any measure of the probability of occurrence, however, such a concept cannot lead to useable rules of liability.[143]

As our brief noted:

> If the Commission adopts [the FTC Staff]'s proposed construction, then every company would be guilty of "exposure of consumers' sensitive personal infor-

[142] Brief of International Center for Law & Economics & TechFreedom as Amici Curiae Supporting Petitioners, *LabMD, Inc. v. Federal Trade Commission*, at 30-31 (11th Cir. Jan. 3, 2017) (No. 16-16270) (*LabMD Amicus Brief)*, http://laweconcenter.org/images/articles/icle-tf-labmd-amicus-final-2017.pdf.

[143] *LabMD IDO* at 82-83; *cf. Int'l Harvester*, 104 FTC 949, 1063 n. 52 (1984).

> mation" if the Commission decides, after the fact, that its data security was "unreasonable" because, according to [the FTC Staff], "an unreasonable failure to protect the information used to commit [identity theft] unquestionably causes or is likely to cause substantial injury.") … This Mobius-strip reasoning would give the Commission unbounded discretion to wield Section 5 against nearly every business in America.[144]

F. Principle #5: Access & Correction

> Users should have qualified access personal data that they have provided, and to rectify, complete, amend, or delete this data. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.[145]

Here, again, appear the concepts discussed above: the importance of the provided/observed/inferred distinction and the need to clearly ground "context" in the FTC's deception doctrine and "risk" in its unfairness doctrine.

One special point bears emphasis: access and correction rights make most sense when applied to information that users provide, rather than information that is observed about them, for at least two reasons.

First, the flipside of any access or correction right is a privacy vulnerability: the possibility that someone other than you may access and maliciously change information about you. To prevent such unauthorized access, obviously, there must be some mechanism for verifying that the person attempting to exercise the access/correction right is, in fact, the data subject. Such a mechanism likely already exists in the vast majority of cases in which users have *provided* information, because such interactions usually involve the creation of an account by a user. Thus, a legal right would not require the creation of new systems to authenticate users — which could raise new privacy concerns, by tying the observation of data about subjects that are generally anonymous to accounts that specifically (even if pseudonymously) identify them.

Second, while it remains possible that a right to correct or delete information, even if that information had been previously provided by the user, could trigger a First Amendment problem (such as when that information involves a matter of public concern), generally, such

---

[144] *LabMD Amicus Brief, supra* note 142 at 4.

[145] *RFC*, *supra* note 6, at 48602.

concerns will be at their nadir when the information involved has been provided by the user themselves.

G. Principle #6: Risk Management

> Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes.[146]

We agree wholeheartedly. Again, the best way to do this is to ground this analysis in Section 5's unfairness analysis — with a meaningful requirement that the Commission establish the risk entailed by a specific practice, rather than the mere *possibility* of harm, as discussed above.

H. Principle #7: Accountability

> Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems. … [E]xternal accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.[147]

That obligations to safeguard data and use it responsibly (i.e., consistent with context and in a manner commensurate with the risks it poses) should flow through from the company that collects it to the other companies to whom it makes data available is, obviously, essential to the functioning of any privacy framework. But this raises the crucial question: what responsibility do companies up the chain of data flows have to assure compliance with companies down the chain? And what responsibility do they have to notify data subjects about misuse of their information by third parties?

We began addressing these difficult questions in a letter we submitted to the relevant Congressional committee leaders in April, after the news broke about Cambridge Analytica's

---

[146] *RFC, supra* note 6, at 48602.

[147] *Id*.

ability to access basic information about the friends of users of an app developed by a researcher associated with the company.[148] We concluded that Facebook's failure to notify users about the misuse of data by Cambridge Analytica could well have constituted a material omission on Facebook's part—and that, regardless, such notifications should, under certain circumstances, be required by a larger statute governing breach notification. On the duty to audit, we concluded:

> Requiring websites to audit every third-party app's use of data, and even every "suspicious app's" use of data, is not only impractical (especially for sites smaller than Facebook); it would also likely prove counter-productive, by distracting limited resources from the most suspicious apps. Imposing such broad liability could significantly disrupt the Internet ecosystem. The burden of such liability would fall hardest not on Facebook but on its smaller competitors. Again, under basic American tort law, even negligent parties cannot be held liable for harm that results from the superseding cause of another's intervention except in narrow circumstances.
>
> In limited circumstances, it could be appropriate for Congress to craft legislation that hold data collectors like Facebook responsible, for preventing the misuse of data collected through their site by third parties—including the transfer of that information (in violation of the terms of service under which it was initially collected by the third party) to fourth parties, who subsequently misuse it. But these circumstances must be narrowly tailored to real harms and clearly defined. For example, where a company has been credibly notified—such as Facebook was by *The Guardian*'s 2015 story—that its data is being misused to influence an American election, and especially where that influence may involve a foreign party, it may be appropriate for that company to have a special duty of care, which could require that the company take additional measures to prevent misuse, such as by requiring an audit to ensure that the data is no longer being used.[149]

Policymakers must proceed with caution here. Holding companies equally responsible for everything their third-party partners do, or for auditing everything they do, could simply encourage companies to consolidate their operations in-house. Instead of working with third-party partners, the largest tech companies would have an incentive to simply acquire those companies or replicate their functionality. Privacy law should *not* drive such vertical integration. Grounding the analysis of what degree of accountability is required (including when audits are required) in the well-established test of Section 5(n) would help to guard

---

[148] TechFreedom, Congressional Letter, *Facebook, Social Media Privacy and the Use and Abuse of Data* and *Facebook: Transparency and Use of Consumer Data,* Hearings before U.S. Senate Committees (Apr. 10, 2018), http://docs.techfreedom.org/TechFreedom_Congressional_Letter-Facebook_hearing_4-10-18.pdf.

[149] *Id*. at 22-23.

against that danger, because the Commission must weigh substantial injury against countervailing benefits to consumers or competition, and the ability to continue sharing information with third party partners who are not under common ownership (and therefore present a greater risk of irresponsible data use) is certainly a significant benefit to competition of not cracking down on data sharing.

VIII. A Privacy Law Modernization Commission

Eventually, some kind of federal data protection legislation *will* pass; it is only a question of time, what that legislation looks like, and how thoughtfully it has been conceived. Given the complexity of the issue, the lack of even a framework through which to understand how to assess how legislation will work in practice, the legislative deadlock in this area since the FTC first requested legislation in 2000, and the lack of expertise in Congress both in technology and difficult questions of administrative law, we are highly skeptical that Congress can resolve this problem on its own. The NTIA can certainly add much clarity to this area by soliciting feedback from interested stakeholders and attempting to distill that input in ways that can inform both the ongoing enforcement of existing consumer protection and privacy-specific laws by the FTC and state attorneys general, as well as Congress in considering updates to American privacy law.

But the most useful thing NTIA could do at this moment would be to recommend to the Administration that it call on Congress to swiftly pass legislation creating a Privacy Law Modernization Commission (PLMC). Such a Commission could draw on two prior models. First, the Fair Information Practice Principles that continue to inform the privacy debate—and from which the principles proposed by NTIA were originally derived—were themselves originally derived from the 1973 report produced by an expert commission chartered by Congress in 1970.[150] Second, in 2002 Congress established the Antitrust Modernization Commission (AMC) to inform its consideration of how to update the competition laws, a situation roughly analogous to that regarding privacy today.[151] The four purposes of the AMC could be adapted for a PLMC with only minor word changes:

> (1) to examine whether the need exists to modernize the antitrust laws and to identify and study related issues;

[150] U.S. Department of Health, Education and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computer, and the Rights of Citizens (1973).

[151] Antitrust Modernization Commission Act of 2002, Pub. L. No. 107-273, §§ 11051-60, 116 Stat. 1856, https://www.congress.gov/bill/107th-congress/house-bill/2325/text .

(2) to solicit views of all parties concerned with the operation of the antitrust laws;

(3) to evaluate the advisability of proposals and current arrangements with respect to any issues so identified; and

(4) to prepare and submit to Congress and the President a report.[152]

A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.

We recommended the creation of precisely such a commission over four years ago, in comments filed with NTIA (along with the International Center for Law & Economics).[153] If our recommendation had been followed, such a Commission would already have completed its work, and we would all benefit from its report — or a majority report and minority report. It is not too late to create such a Commission.

While the AMC was given three years to operate and make its recommendation, we believe a PLMC could conduct its work in much, much less time, given the amount of scholarship in this area and the degree of work already done by the FTC, Commerce Department and other government bodies. We appreciate that California's plan to begin implementing its new legislation in January, 2020, will require tech companies to begin redesigning their systems to come into compliance, and that this creates great urgency for many to see federal legislation passed that would preempt state legislation. The Commission, if convened quickly, could be tasked with producing an initial report and request for comment by, say, the end of the first quarter of 2019, and a final report making recommendations for legislation by summer.

---

[152] *Id*. § 11053.

[153] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 3 (Aug. 5, 2014), http://laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf.

IX. Conclusion

We applaud the NTIA for its undertaking in this complex area. Most important, NTIA is starting at the correct place by defining fundamental principles and precepts, not by jumping immediately into a mode of trying to propose regulations for undefined or under-defined perceived problems. Yet the case for federal legislation, if only to preempt exceptionally sloppy and inconsistent state regulation, is growing, making this issue increasingly urgent.

TechFreedom looks forward to engaging with the NTIA and all stakeholders to help craft a federal privacy policy that protects consumers, but also values innovation, without overburdening an industry that has created an entirely new economy in the past 30 years valued at over a trillion dollars and fast approaching 10% of total U.S. GDP.[154] Cisco estimates that this value may reach $14 trillion within 10 years, with the advent of wholly new uses for the Internet (including the Internet of Things).[155] Above all, policies must not advantage entrenched mature companies who can comply with just about any privacy regime, ahead of the next generation of great innovators, whose Next Killer App must not be strangled in the crib.

[154] *See, e.g.,* Press Release, *New Report Calculates the Size of the Internet Economy,* The Internet Association (Dec. 10, 2015), https://internetassociation.org/121015econreport/.

[155] Frequently Asked Questions, *The Internet of Everything Global Private Sector Economic Analysis*, CISCO, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf.

Comments of

TechFreedom

Hearings on Competition & Consumer Protection in the 21st Century

Topic 2: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks

Berin Szóka,[1] Graham Owens[2] & James E. Dunstan[3]

Overview

TechFreedom is a non-partisan think tank dedicated to promoting the progress of technology that improves the human condition. To this end, we seek to advance public policy that makes experimentation, entrepreneurship, and investment possible, and thus unleashes the ultimate resource: human ingenuity. Wherever possible, we seek to empower users to make their own choices online and elsewhere.

[1] Berin Szóka is President of TechFreedom, a nonprofit, nonpartisan technology policy think tank. J.D. University of Virginia School of Law; B.A. Duke University. He can be reached at bszoka@techfreedom.org.

[2] Graham Owens is a Legal Fellow with TechFreedom. J.D. George Washington University School of Law; B.A. University of Virginia. He can be reached at gowens@techfreedom.org.

[3] James Dunstan is General Counsel of TechFreedom. J.D. Georgetown University Law Center; B.A. Claremont McKenna College. He can be reached at jdunstan@techfreedom.org.

Since its launch in 2011, TechFreedom has spoken often on the FTC's regulation and enforcement of antitrust, unfairness, and consumer protection laws. We welcome the opportunity to once again interact with FTC staff as it works through these issues in a changing world where technological innovation has brought huge benefits to consumers, but has also raised novel questions related to privacy, data security, and unfair business practices.

On June 20, 2018, the FTC announced that the agency will hold a series of public hearings on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy.[4] In preparation for those hearings, the FTC seeks public comment on eleven (11) issues, through the filing of separate comments on each topic. TechFreedom is pleased to submit comments on five (5) of these topics:

- **Topic 1**: The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings[5]
- **Topic 2**: Competition and consumer protection issues in communication, information, and media technology networks[6]
- **Topic 5**: The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters[7]
- **Topic 10**: The interpretation and harmonization of state and federal statutes and regulations that prohibit unfair and deceptive acts and practices[8]
- **Topic 11**: The agency's investigation, enforcement and remedial processes[9]

---

[4] Press Release, Fed. Trade Comm'n, FTC Announces Hearings on Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

[5] Comments of TechFreedom, *Hearings on Competition & Consumer Protection in the 21st Century: Topic 1: The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings* (Aug. 20, 2018), http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshop-comments-topic-1.pdf.

[6] Comments of TechFreedom, *Hearings on Competition & Consumer Protection in the 21st Century: Topic 2: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks* (Aug. 20, 2018), http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshop-comments-topic-2.pdf.

[7] Comments of TechFreedom, *Hearings on Competition & Consumer Protection in the 21st Century: Topic 5: The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters* (Aug. 20, 2018), http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshop-comments-topic-5.pdf.

[8] Comments of TechFreedom, *Hearings on Competition & Consumer Protection in the 21st Century: Topic 10: The interpretation and harmonization of state and federal statutes and regulations that prohibit unfair and deceptive acts and practices* (Aug. 20, 2018), http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshop-comments-topic-10.pdf.

2.c. The application of the FTC's Section 5 authority to the broadband internet access service business

Most of the discussion about how the Federal Trade Commission (FTC) (and state attorneys general) will police the broadband market following the FCC's repeal of the 2015 Open Internet Order (OIO) has focused solely on antitrust law. While antitrust law has a vital role to play in protecting consumers, the principal legal vehicle for addressing net neutrality violations will, in fact, be consumer protection law.

In 2008, following consumer complaints, the FCC found that Comcast delayed or blocked the use of peer-to-peer file-sharing (P2P) applications such as BitTorrent, and that such interference did not constitute reasonable network management.[10] The FTC could likely have brought an enforcement action grounded in deception based on the disconnect between Comcast's content and its claims, once asked by reporters about what the company was doing, that "We're not blocking any access to any application, and we don't throttle any traffic."[11] Comcast repeatedly changed its explanation when confronted with testing evidence.[12] The FTC could also likely have brought an additional deception case: that Comcast's failure to disclose its throttling of BitTorrent traffic before it was caught throttling constituted a material omission. The FTC's failure to bring an enforcement action in this case, its willingness to defer to the FCC, led to the common misperception that the FTC was powerless to act. The FTC must now begin to correct that error by explaining how its existing authority could apply in the case of net neutrality violations.

The FTC's Section 5 authority to police unfair or deceptive practices (UDAP)[13] has regularly been dismissed as inadequate because most commentators assume the FTC's enforcement authority, which is constrained by Section 5's common carrier exception,[14] can do nothing other than enforce the promises ISPs have thus far made—but could cease to make in the

---

[9] Comments of TechFreedom, *Hearings on Competition & Consumer Protection in the 21st Century: Topic 11: The agency's investigation, enforcement and remedial processes* (Aug. 20, 2018), http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshop-comments-topic-11.pdf.

[10] *See In the Matters of Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp.*, WC Docket No. 08-183, Memorandum Opinion and Order, 23 F.C.C. Rcd. 13,028, 13,059 (2008), hraun-foss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf.

[11] *Id.* ¶ 6.

[12] *Id.* ¶¶ 7-9.

[13] 15 U.S.C. § 45.

[14] *Id.* § 45(a)(2) (exempting all "common carriers subject to the Acts to regulate commerce"); *see also* 15 U.S.C. § 44 (defining "Acts to regulate commerce" to mean, inter alia, "the Communication Act").

future—not to block, throttle, prioritize traffic, or engage in other consensus net neutrality violations.[15]

Such claims, however, misunderstand both the nature of the market and the authority the FTC wields under Section 5. In fact, the FTC will be able to enforce not only specific commitments to net neutrality principles (which, yes, companies could potentially change) but also the marketing claims they make more generally, which *imply* adherence to net neutrality principles (and which are unlikely to change). Consider, for example, the lawsuit brought by the New York Attorney General against two cable ISPs for failing to provide network speeds as promised — illustrating that existing consumer protection law, whether applied by state AGs or the FTC, may be able to address potential net neutrality concerns, as discussed below.[16]

The FTC's jurisdiction to bring such cases is now clear again, after the *en banc* decision of the Ninth Circuit, which overruled a panel decision limiting the FTC's authority to police Internet service providers (ISPs) and upheld the FTC's long-standing position that the agency's otherwise general authority excludes common carriers only insofar as they function as such, not because a particular company may be designated as a common carrier.[17] Following the holding and the FCC's reclassification of ISPs as noncommon carriers, the agency can now continue with enforcement actions against AT&T and other ISPs under Section 5.

The FTC's enforcement action against AT&T which prompted that litigation is also particularly illustrative of how the FTC will, now that the jurisdictional issue has been settled, be

---

[15] *See, e.g.*, Gigi Sohn, *The FCC's plan to kill net neutrality will also kill internet privacy*, THE VERGE (Apr. 11, 2017), https://www. theverge.com/2017/4/11/15258230/net-neutrality-privacy-ajitpai-fcc; Anant Raut, *Unlike FCC, FTC cannot protect net neutrality*, THE HILL (Aug. 21, 2017), http://thehill.com/blogs/pundits-blog/ technology/347363-unlike-fcc-ftc-cannot-protect-net-neutrality.

[16] *See* Roslyn Layton & Tom Struble, *Net Neutrality Without the FCC?: Why the FTC Can Regulate Broadband Effectively*, 18 Federalist Soc' Rev. 124, 126 (2017) (citing Press Release, A.G. Schneiderman Announces Lawsuit Against Spectrum-Time Warner Cable and Charter Communications for Allegedly Defrauding New Yorkers Over Internet Speeds and Performance (Feb. 1, 2017), https://goo.gl/ryjX32)). States can not only adequately police broadband providers using their state consumer protection laws generally, given the FCC's express preemption statement, as well as the Dormant Commerce Clause's prohibition on state regulations creating inconsistent rules for the Internet, states *must* use these general laws. *See* Graham Owens, *Federal Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail*, Forthcoming (July 19, 2018), *available at* https://ssrn.com/abstract=3216665 (internal citations omitted).

[17] *Fed. Trade Comm'n v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (holding "FTC Act exemption for common carriers does not bar FTC from regulating such carriers' non-common-carriage activities" and the exemption is "activity-based, meaning that a common carrier is exempt from FTC jurisdiction only with respect to its common-carrier activities").

able to police the broadband market to ensure consumers are protected.[18] The FTC's claim there was based on the marketing claims the company made to attract consumers to buy its products, rather than on the fine print of company's terms of service or its broad statements about net neutrality principles — two entirely distinct potential bases for a deception case. However, though the case began as an investigation into AT&T's marketing claims, as the Ninth Circuit stated, the "central issue [was] one of agency jurisdiction and statutory construction" as to how the Commission can regulate broadband.[19]

AT&T began marketing "unlimited" data plans in 2007, but ceased to do so in June 2010, when the company began offering "tiered" data plans instead, while offering to grandfather consumers with "unlimited" plans.[20] In July 2011, Critically, the company "began reducing the data speed for its unlimited mobile data plan customers—a practice commonly referred to as 'data throttling.'"[21] According to the FTC's complaint, the company's practice was unfair and deceptive because the company repeatedly promised consumers unlimited mobile data, "but in fact imposed restrictions on data speed for customers who exceeded a present limit,"[22] stating:

> When it implemented its throttling program, Defendant possessed internal focus group research indicating that its throttling program was inconsistent with consumer understanding of an "unlimited" data plan. The researchers concluded that, "[a]s we'd expect, the reaction to [a proposed data throttling program] was negative; consumers felt 'unlimited should mean unlimited [.']" The focus group participants thought the idea was "clearly unfair." The researchers highlighted a consumer's comment that "[i]t seems a bit misleading to call it Unlimited." The researchers observed that "[t]he more consumers talked about it the more they didn't like it." This led the researchers to advise that "[s]aying less is more, [so] don't say too much" in marketing communications concerning such a program.[23]

Other cases also illustrate the types of protections the FTC can provide for consumers. In addition to the action against AT&T for misleading customers as to the realities of its "unlimited" data plan, the FTC separately was able to require AT&T to pay "$88 million in re-

---

[18] *See* Press Release, Fed. Trade Comm'n, *FTC Says AT&T Has Misled Millions of Consumers with 'Unlimited' Data Promises* (Oct. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/10/ftc-says-att-has-misled-millions-consumers-unlimited-data.

[19] *AT&T Mobility LLC*, 883 F.3d at 850.

[20] *Id*. at 851.

[21] *Id*.

[22] *Id*.

[23] Complaint at 5, FTC v. AT&T Mobility LLC, 87 F. Supp. 3d 1087 (N.D. Cal. 2015), https://www.ftc.gov/system/files/documents/cases/141028attcmpt.pdf.

funds to more than 2.7 million AT&T customers who had third-party charges added to their mobile bills without their consent, a tactic known as 'mobile cramming.'"[24] In an action almost identical to the one brought against AT&T for false promises of "unlimited data," the FTC also successfully brought an action against Tracfone, the largest prepaid mobile provider in the U.S., with Tracfone agreeing to pay $40 million to the FTC for consumer redress.[25]

As these cases illustrate, not only does the FTC have the authority and expertise to police the broadband market to protect consumers, as former Commissioner Josh Wright made clear to Congress, the Commission also has powers to make consumers whole that are unavailable to the FCC:

> Importantly, the FTC has certain enforcement tools at its disposal that are not available to the FCC. Unlike the FCC, the FTC can bring enforcement cases in federal district court and can obtain equitable remedies such as consumer redress. The FCC has only administrative proceedings at its disposal, and rather than obtain court- ordered consumer redress, the FCC can require only a "forfeiture" payment. In addition, the FTC is not bound by a one-year statute of limitations as is the FCC. The FTC's ability to proceed in federal district court to obtain equitable remedies that fully redress consumers for the entirety of their injuries provides comprehensive consumer protection and can play an important role in deterring consumer protection violations.[26]

Enforcement of Corporate Promises

Today, every major ISP has promised not to violate net neutrality principles[27] in prominent, repeated and clear statements to the public. For example, AT&T has been unequivocal in its commitment to an open internet:

---

[24] Press Release, FTC Providing Over $88 million in Refunds to AT&T Customers Who Were Subjected to Mobile Cramming (Dec. 8, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/ftc-providing-over-88-million-refunds-att-customers-who-were.

[25] Press Release, Fed. Trade Comm'n, Prepaid Mobile Provider TracFone to Pay $40 Million to Settle FTC Charges It Deceived Consumers About 'Unlimited' Data Plans (Jan. 28, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/prepaid-mobile-provider-tracfone-pay-40-million-settle-ftc.

[26] Joshua D. Wright, *Wrecking the Internet to Save it? The FCC's Net Neutrality Rule*, Testimony Before the U.S. House of Representatives, Committee on the Judiciary at 17 (Mar. 25, 2015), https://judiciary.house.gov/wp-content/uploads/2016/02/Wright-Testimony-1.pdf (internal citations omitted).

[27] *See Net Neutrality and the Role of Antitrust: Hearing Before the Subcomm. On Reg. Reform, Commercial and Antitrust Law of the H. Comm. on the Judiciary*, 115th Cong. (2018) (testimony of Maureen Ohlhausen, Acting Chairman, Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1268913/commission_testimony_re_net_n

> AT&T is committed to an open internet. *We don't block websites. We don't censor online content. And we don't throttle, discriminate, or degrade network performance based on content*. Period.
>
> We have publicly committed to these principles for over 10 years. And we will continue to abide by them in providing our customers the open internet experience they have come to expect.[28]

Other leading ISPs have made similar claims:

1. **Comcast**: "*We do not block, slow down or discriminate against lawful content*. We believe in full transparency in our customer policies. We are for sustainable and legally enforceable net neutrality protections for our customers."[29]
2. **Verizon**: "**Full Access**: We will not block any legal internet content, applications, or services based on their source or content. **Full Speed**: We will not throttle or slow down any internet traffic based on its source or content. **Fair Handling of Traffic**: We will not accept payments from any company to deliver its traffic faster or sooner than other traffic on our consumer broadband service, nor will we deliver our affiliates' internet traffic faster or sooner than third parties'. We will not prioritize traffic in a way that harms competition or consumers."[30]
3. **Cox Communications**: "Cox remains committed to providing an open internet experience for customers that is consistent with net neutrality principles. Shifts in how internet services are classified by regulators does not change our commitment. *We do not block, throttle, or otherwise interfere with consumers' desire to go where they want on the internet*. Congress should enact permanent bipartisan legislation that

---

eutrality and the role of antitrust 11012017.pdf (outlining the key concerns raised by supporters of net neutrality regulations).

[28] Randall Stephenson, *Consumers Need an Internet Bill of Rights*, AT&T (January 24, 2018), http://about.att.com/story/consumers need an internet bill of rights.html.

[29] Comcast Statement, *Comcast is Committed to an Open Internet*, COMCAST (last visited August 20, 2018 4:00PM), https://corporate.comcast.com/openinternet/open-net-neutrality.

[30] *See Verizon, Our Commitment to Broadband Consumers*, VERIZON (last visited August 20, 2018 4:02PM), https://www.verizon.com/about/our-company/verizon-broadband-commitment ; *see also* Verizon, *Verizon Supports FCC's Restoring Internet Freedom Proposal*, (November 21, 2017), https://www.verizon.com/about/news/verizon-supports-fccs-restoring-internet-freedom-proposal ("we continue to strongly support net neutrality and the open internet. Our company operates in virtually every segment of the internet. We continue to believe that users should be able to access the internet when, where, and how they choose, and our customers will continue to do so.").

guarantees protections for consumers, applies equally to all internet companies and ends the regulatory uncertainty that occurs with every administration change."[31]

The FTC will have little difficulty enforcing these promises via its deception authority—even if it were to accept our advice concerning the need to more clearly define materiality.[32] All of these companies have gone to great lengths to publicize these marketing claims, solemnly calling them "commitments" to consumers. AT&T even went so far as to take out full page ads in major papers across the country making that commitment clear.[33]

Clarification of How the FTC Will Interpret Corporate Promises

Despite the lack of equivocation in the commitments made by such leading ISPs to respect net neutrality, the FTC could face complex questions of fact in policing conduct by such a company: what, precisely, do such commitments mean in principle? We think these questions will, and should, be resolved under the same analytic framework laid out by the FCC's 2010 and 2015 Open Internet Orders, which grappled with these issues — most notably, the definition of the word "reasonable" in "reasonable network management," which functions as an exception to the blocking and throttling rules.[34]

The agency has essentially two options to address such issues: clarification *ex post* (case-by-case), or some form of *ex ante* guidance. Despite our general preference for *ex post* approaches, we believe there is ample consensus about the meaning of reasonable network management, at least at the conceptual level on which *ex ante* guidance can be provided. Even with *ex ante* clarification, thorny questions will inevitably arise about the meaning of these standards in the FTC's enforcement work, just as such questions arose for the FCC. For example, did the FCC's 2015 ban on throttling apply to T-Mobile's Binge On program, as EFF alleged, because it allegedly "throttled" the entire class of video traffic — even though users could easily toggle Binge On on and off?[35]

---

[31] Cox, *Net Neutrality,* COX (last visited August 20, 2018 4:05PM), https://www.cox.com/residential/support/net-neutrality.html.

[32] *See infra* at 16-17.

[33] AT&T Blog Team, *Consumers Need an Internet Bill of Rights*, AT&T (January 24, 2018), https://www.attpublicpolicy.com/consumer-broadband/consumers-need-an-internet-bill-of-rights/.

[34] *In re Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 29 FCC Rcd 5561 ¶¶ 214-224 (2015) (JA 3477-8876), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

[35] Jeremy Gillula, *EFF Confirms: T-Mobiles Binge On is Just Throttling, Applies Indiscriminately to All Video*, EFF (January 4, 2016), https://www.eff.org/deeplinks/2016/01/eff-confirms-t-mobiles-bingeon-optimization-just-throttling-applies.

We believe the FTC should issue a Policy Statement to address these questions at a level of generality comparable to that contained in the FCC's 2015 Open Internet Order — *i.e.*, defining blocking, throttling, prioritization and reasonable network management. The more difficult questions left out of the FCC's rules, and addressed instead in the Order itself, should likewise be left out of any FTC policy statement — and left for development by the FTC and state attorneys general applying the same UDAP authority.

Enforcement of Self-Regulatory Codes & Arbitration of Disputes

Those skeptical of the FTC's ability to police the broadband market seem to have focused on three alleged inadequacies of the promises made thus far by broadband companies: (1) that they are not uniform, varying from company to company; (2) that they are insufficiently detailed; and (3) that they could be changed at a whim. All three problems could be addressed by the development of a code of conduct adhered to by industry. While we are leery of the government leaning on private companies to develop codes of conduct, this case is unusual, given the degree of consensus around the underlying principles and the unique sensitivity of the issue. At a minimum, it would be helpful for the FTC Chairman to urge broadband providers to consider developing such a code of conduct themselves.

Even more helpful to the FTC than the development of a common self-regulatory code would be the creation of a forum with sufficient technical expertise and objectivity to address disputes over alleged net neutrality violations as they arise. We believe the Broadband Internet Technical Advisory Group (BITAG) could be the catalyst for such a forum, as it already represents a unique cross-section of the companies potentially involved in such disputes, including ISPs, edge companies and other middlemen between the two.

2.d. Unique competition and consumer protection issues associated with internet and online commerce

Bias / Neutrality of "Platform" Companies

A critical consumer protection issue unique to the Internet and online commerce that the FTC must address is how social media platforms—such as Facebook and Twitter—moderate the content on their websites. This issue is critical to the FTC for two reasons: (1) to ensure that social media platforms are open and honest to consumers about how and why they remove certain content, and (2) to ensure consumers are not deprived of innovative technologies and information due to overly restrictive, and potentially unconstitutional, regulations imposed by lawmakers that believe such platforms are not neutral and discriminatorily removing conservative content. Indeed, as the concern over social media plat-

forms' "neutrality," corporate promises made that such platforms are neutral, and how the FTC might enforce such promises greatly resembles the net neutrality issue above, this point is particularly critical for the FTC to address. However, to understand this two-part issue and how it uniquely affects online commerce, it's important to understand the background of the underlying issue and history of social media content regulation.

1. Background of Media Bias Concerns and the Fairness Doctrine

Concern over "media bias" and fairness itself is not a new issue in the United States. From 1949 until President Reagan finally abolished it in the 1980s, the Federal Communications Commission (FCC) imposed strict rules on broadcast media in an attempt to prevent bias known as the "Fairness Doctrine."[36] Initially laid out in the report *In the Matter of Editorializing by Broadcast Licensees*, the Fairness Doctrine was based on the FCC's belief that "the public interest requires ample play for the free and fair competition of opposing views, and the commission believes that the principle applies to all discussion of importance to the public."[37] Under the Fairness Doctrine, the FCC required broadcast licensees to "adequately cover issues of public importance" and to ensure that "the various positions taken by responsible groups" were aired.[38] In practice, this meant that licensees were obligated to give air time on demand to anyone seeking to voice an alternative opinion, or to reply to an "attack."[39]

Despite the clear First Amendment concerns associated with regulating private companies' content, in 1969 the Supreme Court upheld the doctrine in *Red Lion Broadcasting Co. v. FCC*.[40] After journalist Fred Cook criticized Republican Presidential nominee Barry Goldwater during the 1964 campaign, a radio station owned by the Red Lion Broadcasting Corporation aired a program making several defamatory claims about Cook, most notably that he had been working for a Communist publication.[41] The FCC's personal attack rules made broadcasters responsible for giving the person attacked "a tape, transcript, or summary" of the broadcast to that public figure and offer that person a reasonable opportunity to reply

---

[36] Thomas J. Houser, *The Fairness Doctrine—An Historical Perspective,* 47 Notre Dame L. Rev. 550 (1972), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=2935&context=ndlr.

[37] In the Matter of Editorializing by Broadcast Licensees, 13 F.C.C. 1246 (1949).

[38] *Id*. at 1249; accord United Broad. Co., 10 F.C.C. 515, 517 (1945); Cullman Broad. Co., 40 F.C.C. 576, 577 (1963).

[39] Broadcast Procedure Manual, 49 F.C.C.2d at 6 (1974); *see also* Thomas J. Houser, *The Fairness Doctrine—An Historical Perspective,* 47 Notre Dame L. Rev. 550 (1972), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=2935&context=ndlr.

[40] *Red Lion Broadcasting Co. v. F.C.C.*, 395 U.S. 367 (1969).

[41] *Id*.

— for free if necessary.[42] Justice White, writing for a unanimous court, emphasized the unique nature of broadcasting, as evident to Congress in enacting the Federal Radio Commission in 1927: "It quickly became apparent that broadcast frequencies constituted a scarce resource whose use could be regulated and rationalized only by the Government. Without government control, the medium would be of little use because of the cacophony of competing voices, none of which could be clearly and predictably heard."[43] On this factual finding turned the outcome of the case: "Although broadcasting is clearly a medium affected by a First Amendment interest, differences in the characteristics of new media justify differences in the First Amendment standards applied to them."[44]

However, in upholding the doctrine, the *Red Lion* Court nonetheless cautioned that, "if experience with the administration of these doctrines indicates that they have the net effect of reducing, rather than enhancing, the volume and quality of coverage, there will be time enough to reconsider the constitutional implications."[45] The FCC did study the issue and, in 1985, found just such chilling effects,[46] and just two years later effectively abolished the Fairness Doctrine.[47] Congress, then controlled by Democrats, passed legislation to restore the Fairness Doctrine.[48] President Reagan vetoed the bill, declaring, "[t]his type of content-based regulation by the federal government is, in my judgment, antagonistic to the freedom of expression guaranteed by the First Amendment. In any other medium besides broadcasting, such federal policing of the editorial judgment of journalists would be unthinkable."[49] President Reagan continued:

> The Supreme Court indicated in *Red Lion* a willingness to reconsider the appropriateness of the fairness doctrine if it reduced rather than enhanced broadcast

---

[42] Billings Broad. Co., 40 F.C.C. 518, 520 (1962).

[43] *Red Lion*, 395 U.S. at 376.

[44] *Id.* at 387.

[45] *Id*. at 393.

[46] General Fairness Doctrine Obligations of Broadcast Licensees, Report, 50 Fed. Reg. 35418 (1985), https://ia800204.us.archive.org/24/items/FairnessReport/102Book1FCC2d145.pdf; see also Mark A. Conrad, The Demise of the Fairness Doctrine: A Blow for Citizen Access, 41 FED. COMM. L.J. 161, 176 (1989) ("Regarding the First Amendment, the 1985 report displayed doubts about the Doctrine's constitutionality, believing it 'chills' speech and requires the government to act as a de facto censor.").

[47] In Re Complaint of Syracuse Peace Council against TV Station WTVH Syracuse, N.Y., Memorandum Opinion and Order, 2 FCC Rcd. 5043, para. 82 (1987), recons. denied, 3 FCC Red. 2035 (1988), aff'd sub nom. Syracuse Peace Council v. FCC, 867 F.2d 654 (D.C. Cir. 1989), cert. denied, 493 U.S. 1019 (1990).

[48] Fairness in Broadcasting Act of 1987. H.R. 1937, 100th Cong., 1st Sess. (1987); S. 742, 100th Cong., 1st Sess. (1987).

[49] Veto of Fairness in Broadcasting Act of 1987, 133 Cong. Rec. 16989 (June 23, 1987), http://www.presidency.ucsb.edu/ws/?pid=34456.

> coverage. In a later case, the Court acknowledged the changes in the technological and economic environment in which broadcasters operate. It may now be fairly concluded that the growth in the number of available media outlets does indeed outweigh whatever justifications may have seemed to exist at the period during which the doctrine was developed. The FCC itself has concluded that the doctrine is an unnecessary and detrimental regulatory mechanism. After a massive study of the effects of its own rule, the FCC found in 1985 that the recent explosion in the number of new information sources such as cable television has clearly made the "fairness doctrine" unnecessary. Furthermore, the FCC found that the doctrine in fact inhibits broadcasters from presenting controversial issues of public importance, and thus defeats its own purpose.[50]

President Reagan made clear, as the FCC itself had done in its 1985 report, that the original rationale for the Fairness Doctrine rested on shaky constitutional foundations regardless of the scarcity of broadcast spectrum or the degree of competition on the airwaves:

> Quite apart from these technological advances, we must not ignore the obvious intent of the First Amendment, which is to promote vigorous public debate and a diversity of viewpoints in the public forum as a whole, not in any particular medium, let alone in any particular journalistic outlet. History has shown that the dangers of an overly timid or biased press cannot be averted through bureaucratic regulation, but only through the freedom and competition that the First Amendment sought to guarantee.[51]

2. Media Bias Concerns & the Threat of an Internet Fairness Doctrine

From the Fairness Doctrine's inception in 1949 to its abolition in 1987, and even as recently as 2016, Republicans and free-market proponents opposed this doctrine, arguing that it was not "free," stifled conservative voices in the media, and violated the First Amendment by controlling the content private companies' reported on.[52] Indeed, opposition to the Fairness Doctrine has been in every Republican party platform since 2008.[53] Yet, despite this almost half-century fight against government regulation of speech in media, Republicans made an about face over the past year arguing that the government should step in and

---

[50] *Id*.

[51] *Id*.

[52] *Filtering Practices of Social Media Platforms, Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 2-3 (2018) (testimony of Berin Szóka, President, TechFreedom), https://judiciary.house.gov/wp-content/uploads/2018/04/Szoka-Testimony.pdf [hereinafter Szóka Testimony, *Filtering Practices of Social Media*].

[53] *Id*. at 3.

police the "neutrality" of websites due to a belief that social media websites discriminate against conservatives in managing their content.[54]

For example, in a recent hearing featuring Facebook CEO Mark Zuckerberg, Senators Ted Cruz (R-TX) and Lindsay Graham (R-SC) argued that social media platforms must remain "neutral" in filtering their content despite being private companies, with Sen. Graham stating, "[Website operators] enjoy liability protections because they're neutral platforms. At the end of the day, we've got to prove to the American people that these platforms are neutral."[55] To illustrate that the Senators' belief that the First Amendment somehow applies to private entities, Sen. Graham reportedly proposed a task force made up of members of the Senate Commerce and Judiciary committees to investigate this issue and make concrete proposals on how to regulate social media platforms.[56]

The House Judiciary Committee similarly convened multiple hearings "examining social media filtering practices and their effect on free speech" and discussing ways Congress could police the "neutrality" of websites just as the FCC policed broadcasters under the Fairness Doctrine.[57] Ironically, Chairman Bob Goodlatte (R-VA), invoked the Fairness Doctrine's abolition *in support* of holding such hearings: "Speaking before the Phoenix Chamber of Commerce in 1961, Ronald Reagan observed that, 'freedom is never more than one generation away from extinction.'"[58] This was ironic because, of course, President Reagan was arguing *against* government meddling in media.

---

[54] *See, e.g., id*. (statement of Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary) ("However, beyond illegal activity, as private actors, we know that these companies manage content on their platforms as they see fit. The First Amendment offers no clear protections for users when Facebook, Google, or Twitter limits their content in any way…. There is, however, a fine line between removing illegal activity and suppressing speech. And while these companies may have legal, economic, and ideological reasons to manage their content like a traditional media outlet, we must nevertheless weigh as a nation whether the standards they apply endanger our free and open society and its culture of freedom of expression, especially when it is through these channels that our youth are learning to interact with each other and the world.").

[55] *Facebook, Social Media Privacy, and the Use and Abuse of Data: J. Hearing of S. Comm. on the Judiciary and S. Comm. on Commerce, Science, and Transp*., 115th Cong. (2018) (statement of Sen. Lindsay Graham, Member, S. Comm. on Commerce, Science, and Transp.), http://www.cruz.senate.gov/?p=video&id=3715.

[56] *See* Elena Schor, *Graham seeks 9/11-style commission on social media vulnerabilities*, POLITICO (Nov. 2, 2017), https://www.politico.com/story/2017/11/02/social-media-commission-lindsey-graham-244466.

[57] *See, e.g., Filtering Practices of Social Media*, *supra* note 52; *Facebook, Google and Twitter: Examining the Content Filtering Practices of Social Media Giants Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2018), https://judiciary.house.gov/hearing/facebook-google-and-twitter-examining-the-content-filtering-practices-of-social-media-giants/;

[58] *Filtering Practices of Social Media Platforms, Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2018), https://judiciary.house.gov/press-release/goodlatte-opening-statement-on-social-media-filtering/ (statement of Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary).

President Trump has been even more forceful in his attacks, recently alleging social media companies are discriminating against prominent conservatives, saying: "we won't let that happen."[59] "Social Media is totally discriminating against Republican/Conservative voices. Speaking loudly and clearly for the Trump Administration, we won't let that happen. They are closing down the opinions of many people on the RIGHT, while at the same time doing nothing to others....." the president tweeted.[60] ".....Censorship is a very dangerous thing & absolutely impossible to police. If you are weeding out Fake News, there is nothing so Fake as CNN & MSNBC, & yet I do not ask that their sick behavior be removed. I get used to it and watch with a grain of salt, or don't watch at all."[61]

Why conservatives would suddenly embrace the Fairness Doctrine after decades of opposing it is simply baffling. Conservative talk radio was impossible before the Reagan FCC repealed the Fairness Doctrine, for example. The Fairness Doctrine suppressed heterodox viewpoints and enforced a bland orthodoxy in media and imposing similarly rigid rules would not only do the same for the Internet, but likely impose two kinds of costs far more harmful to consumers.

First, imposing a Fairness Doctrine on the Internet would stifle innovation and competition within the social media marketplace, thereby removing the very threat best able to keep large social media platforms in check: disruptive startups seeking to steal Facebook and Twitter's market share. Ultimately, the best check on incumbent social media giants is the threat of the next startup capable of disrupting these companies' dominance — just as many younger Internet users abandoned Facebook first for Instagram and then for Snapchat. Regulators should avoid creating vague legal liability, not least because, while it might be manageable for a company as large and well-resourced as Facebook, which has thousands of employees working just in content moderation,[62] it will be fatal to the startups

---

[59] Donald Trump (@realdonaldtrump), Twitter (August 18, 2018, 7:23), https://twitter.com/realDonaldTrump/status/1030777074959757313; *see also* Politico Staff, *'We won't let that happen:' Trump alleges social media censorship of conservatives,* POLITICO (Aug. 18, 2018), https://www.politico.com/story/2018/08/18/trump-social-media-censorship-conservatives-twitter-facebook-787899.

[60] *Id*.

[61] Donald Trump (@realdonaldtrump), Twitter (August 18, 2018, 7:32), https://twitter.com/realDonaldTrump/status/1030779412973846529.

[62] *See, e.g.,* Hayley Tsukayama, *Facebook adds 3,000 employees to screen for violence as it nears 2 billion users*, WASHINGTON POST (May 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/05/03/facebookis-adding-3000-workers-to-look-for-violence-on-facebook-live/?utm_term=.8d729c427ada.; Anita Balakrishnan, *Facebook pledges to double its 10,000-person safety and security staff by end of 2018*, CNBC (Oct. 31, 2017), https://www.cnbc.com/2017/10/31/facebook-senate-testimony-doubling-security-group-to-20000- in-2018.html (citing Congressional testimony by Facebook VP and General Counsel Colin Stretch).

seeking to become the next Facebook.[63] Finally, not only would imposing a Fairness Doctrine on the Internet stifle innovation, but it would also stifle competition among platforms, the only means of controlling the speech of private businesses the Supreme Court says is allowed by the First Amendment: "'Under the First Amendment there is no such thing as a false idea,' and the only way that ideas can be suppressed is through 'the competition of other ideas.'"[64]

Second, an Internet Fairness Doctrine would suppress the very free flow of information upon which the Supreme Court held free-enterprise depends by imposing content-based restrictions on private businesses.[65] Despite claims to the contrary by Republican lawmakers, such regulations would be unconstitutional despite *Red Lion* and social media platforms do not qualify as "state actors" subject to the First Amendment.[66] In *Brown v. EMA*, the Court made so much clear by not only extended full First Amendment protection to video games, but declaring that it will do so for all new media:

> Like the protected books, plays, and movies that preceded them, video games communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world). That suffices to confer First Amendment protection. Under our Constitution, "esthetic and moral judgments about art and literature . . . are for the individual to make, not for the Government to decree, even with the mandate or approval of a majority." United States v. Playboy Entertainment Group, Inc., 529 U. S. 803, 818 (2000). And ***whatever the challenges of applying the Constitution to ever-advancing technology, "the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary" when a new and different medium for communication appears***.[67]

3. What the FTC Can, and Should, Do

Suppression of both innovation and the free flow ideas should be of great concern to the FTC as both would greatly harm consumers. For this reason, the FTC should utilize these

---

[63] *See* D. Wakabayashi & A. Satariano, *How Looming Privacy Regulations May Strengthen Facebook and Google*, NEW YORK TIMES (April 28, 2018), https://www.nytimes.com/2018/04/23/technology/privacy-regulationfacebook-google.html.

[64] *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc*., 425 U.S. 748, 780 (1976) (quoting *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 340 (1974)).

[65] *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc*., 425 U.S. 748 (1976).

[66] *See* Szóka Testimony, *Filtering Practices of Social Media* at 17-21, *supra* note 52.

[67] *Brown v. Entm't Merchants Ass'n*, 564 U.S. 786, 790 (2011) (quoting *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 503 (1952)) (emphasis added).

hearings to simultaneously address any concern regarding social media bias and make clear to the public and lawmakers alike that, under Section 5, the FTC already has the authority to address this issue through other measures, starting with transparency and user empowerment, without stifling innovation or suppressing free speech. Doing so would greatly benefit consumers by (1) ensuring that social media platforms are open and honest to consumers about how and why they remove certain content, and (2) ensuring consumers are not deprived of innovative technologies and information due to overly restrictive, and potentially unconstitutional, regulations imposed by lawmakers that believe such platforms are discriminatorily removing conservative content.

It is extremely unlikely that any court would ever decide that Facebook, Twitter or such social networks are state actors under any Supreme Court precedent.[68] Since social media networks are private entities not subject to the First Amendment, the real concern for the government should be whether such platforms are being honest and transparent with consumers as to how they manage content on their platforms. For this reason, the most productive way to go about addressing bias concerns is by focusing on transparency and user empowerment so users better understand these platforms' policies so they, as consumers, can make educated decisions about which platforms to use or not use (the greatest deterrent is always lost profits or the threat of competitor unseating them).

As private entities, social media platforms are free--constitutionally and under Section 230[69]—to remove any content or ban any users they wish; however, if such platforms claim they in no way discriminate against right-leaning users, but in fact are discriminating, then such an act likely constitutes a deceptive practice under Section 5.[70] Under Section 5, which prohibits "deceptive acts or practices in or affecting commerce," an act or practice is deceptive where: "a representation, omission, or practice misleads or is likely to mislead a consumer"; "a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances"; and "the misleading representation, omission, or practice is material."[71] Congress intentionally framed the FTC's authority under Section 5 in the general terms "unfair" and "deceptive" for exactly this purpose: to en-

[68] *See* Szóka Testimony, *Filtering Practices of Social Media* at 19-21, *supra* note 52, for a lengthy analysis of why social media platforms are not state actors.

[69] 47 U.S.C. § 230(c)(2)(A).

[70] 15 U.S.C. § 45.

[71] *See* Federal Reserve, *Consumer Compliance Handbook: Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices* 1 (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

sure that the agency could protect consumers and competition throughout all trade and under changing circumstances.[72]

Using Twitter's policies and statements from its CEO, for example, it is easy to see how the FTC could use Section 5 to address concerns of bias through transparency and user empowerment. Twitter's policy expressly states that it doesn't moderate content:

> People are allowed to post content, including potentially inflammatory content, as long as they're not violating the Twitter Rules. It's important to know that *Twitter does not screen content or remove potentially offensive content*. As a policy, *we do not mediate content or intervene in disputes between users*. However, targeted abuse or harassment may constitute a violation of the Twitter Rules and Terms of Service.[73]

Further, to remove any doubt on this point, CEO Jack Dorsey made clear "we are not" removing content "according to political ideology or viewpoints."[74] Dorsey continued, "We do not look at content with regards to political viewpoint or ideology. We look at behavior."[75]

Should President Trump or Rep. Goodlatte's concerns about Twitter removing content based on users' conservative political ideology be substantiated, such clear statements by Twitter and its CEO could easily serve as the basis for bringing a deception claim against the company in the same way it can enforce promises of neutrality made by ISPs.[76] Since the FTC is already empowered to police any such deceptive acts or practices, and to investigate potentially deceptive practices, there is simply no need for regulators to create vague legal liability through an Internet Fairness Doctrine that would stifle innovation and suppress speech — even if such a doctrine were constitutional, which it most definitely is not.[77]

---

[72] *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (observing if Congress "were to adopt the method of definition, it would undertake an endless task").

[73] Twitter, *About offensive content* (last visited Aug. 18, 2018), https://help.twitter.com/en/safety-and-security/offensive-tweets-and-content (emphasis added).

[74] Brian Stetler, *Twitter's Jack Dorsey: 'We are not' discriminating against any political viewpoint*, CNN (Aug. 18, 2018), https://money.cnn.com/2018/08/18/media/twitter-jack-dorsey-trump-social-media/index.html.

[75] *Id*.

[76] *See supra* notes 27-35 and associated text.

[77] *See* Szóka Testimony, *Filtering Practices of Social Media* at 19-21, *supra* note 52, for a lengthy analysis of why social media platforms are not state actors.

Deception: The Definition of Materiality

In the pre-Internet era, companies generally made (or omitted to make) two kinds of claims to consumer that the FTC policed via its deception authority: (1) marketing claims, usually in the form of print, television, radio or billboard advertisements and (2) warranties. The Digital Revolution changed the way consumers interact with companies, offering wholly new channels for communication, from online help pages and FAQs to direct (and public) interaction on Twitter and Facebook. In addition, every tech company now has terms of service and privacy policies that summarize what kinds of data they collect, how they use it, how they secure it, and much more. The FTC's basic mission in applying its Deception authority—to ensure that consumers get the benefit of the bargain—but *how* to do that that has become considerably more complicated.

The FTC's analysis of deception turns on whether a statement (or omission) was *material* to the consumer. If so, and if the consumer did not get that promised attribute of the product, the Commission may infer that the consumer has been injured—and avoiding unjustified consumer injury is the overall purpose of the FTC Act—*without having to establish injury directly*. Materiality, then, serves as analytical proxy for consumer injury. The FTC's 1983 Deception Policy Statement allows a second analytical proxy: the FTC may presume materiality (and thus injury) when a misstatement has been in "express claims." This shortcut made sense in the context of traditional advertising and warranties, but no longer makes sense in the online environment, where not every "statement" made by companies is, like an advertisement, intended to convince the consumer to buy the product.

We explain this issue in greater depth in our 2016 white paper (co-authored with the International Center for Law & Economics),[78] and in even greater detail in our 2015 white paper about the *Nomi* case (also co-authored with ICLE).[79] In the former, we make the following recommendations to Congress and the FTC:

1. Congress should codify the Deception Policy Statement in a new Section 5(o) and/or the FTC should produce a Policy Statement on Materiality; in either case, when materiality can be presumed should be clarified;

---

[78] *See* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE 57-60 (2016), http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf [hereinafter *White Paper*] at 21-28.

[79] Comments of TechFreedom & International Center for Law and Economics, *In the Matter of Big Data and Consumer Privacy in the Internet Economy,* Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf

2. In particular, Congress or the FTC should clarify that legally mandated language (such as privacy policy statements) cannot be presumed to be material; and
3. A preponderance of the evidence should apply in non-fraud deception cases.

Unfairness: Cost-Benefit Analysis in General

After the FTC's regulatory bender of the late 1970s, using "unfairness" to prohibit whatever practices the Commission decided offended public policy, and the agency's cataclysmic confrontation with Congress in 1980, the Commission effectively ceased using unfairness except for a few categories of unambiguously harmful conduct.[80] Only in the late 1990s, as the Commission began grappling with data brokers and the Internet, did the Commission begin using unfairness again. Within a few years, the Commission had begun building a "common law of consent decrees" based on unfairness — but without the development of the meaning of unfairness by courts anticipated by the 1980 Unfairness Policy Statement, which declared:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion.[81]

Our 2016 white paper made two key suggestions to clarify the meaning of unfairness:[82]

- We support Rep. Markwayne Mullin's (R-OK) bill (H.R. 5115), which would further **codify** promises the FTC made in its 1980 Unfairness Policy Statement; and
- A **preponderance of the evidence** requirement should apply to all complaints based on unfairness.

Unfairness & Deception: Product Design Issues

The Digital Revolution has created a particular kind of consumer protection issue that we expect will arise more and more in the Commission's work: whether user interface design—from ads to websites to the displays on gadgets—is deceptive or unfair. The Commission began dealing with these issues in earnest in the trio of cases it brought concerning

---

[80] *See generally Beales*, *supra* note 17.

[81] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (hereinafter 1980 Unfairness Policy Statement).

[82] White Paper at 15-21.

purchases made by children without their parents' authorization because of the design of the app stores offered by Apple, Google and Amazon.[83]

Of course, this *could* be a proper, indeed highly valuable, exercise of the Commission's authority. Yet it is also fraught with peril: no one wants the FTC to get into the business of designing software or websites, as the European Commission has done through its antitrust actions against Microsoft (requiring the infamous browser ballot to be included in Windows[84]) and Google (dictating how additional results can be displayed alongside standard "ten blue links" search results[85]). If, as the old joke goes, a camel is a horse design by committee, just imagine what an Internet designed by a government agency might look like!

The problem is that the Commission could start sliding down this slippery slope all too easily, settling one enforcement action at a time turning on, and ultimately prescribing, user interface design, while earnestly and sincerely disclaiming any intention of grabbing the digital brush, so to speak, from user interface experts. If the British Empire was acquired "in a fit of absence of mind," so, too, might one say that the FTC created a common law of privacy and data security through a series of consent decrees — without *any* adjudication from the courts as to the proper limits of the FTC's authority envisioned under, or the kind of cost-benefit analysis required by, the Unfairness Policy Statement.[86]

Realizing this danger, as well as the inevitability of the Commission having to deal with legitimate consumer protection concerns turning on product design, we urge the Commission to consider developing, after a thorough public discussion of this issue, a policy statement to guide how the agency will deal with these issues in the future. Most fundamentally, the Commission should make clear that it will not lightly second-guess user interface design decisions (in finding liability), nor will it impose its own judgments about the specifics

---

[83] Press Release, Fed. Trade Comm'n, Apple Inc. Will Provide at least $32.5 Million to Settle FTC Complaint It Charged for In-App Purchases Without Parental Consent (January 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million; Press Release, Fed. Trade Comm'n, FTC Approves Final Order in Case About Google Billing for Kid's In-App Charges without Parental Consent (December 5, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-case-about-google-billing-kids-app; Press Release, Fed. Trade Comm'n, FTC Alleges Amazon Unlawfully Billed Parents For Millions of Dollars in Children's Unauthorized In-App Charges (July 10, 2014), https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars.

[84] Zach Whitaker, *Microsoft 'to comply' with EU in browser choice antitrust probe*, CNET (September 8, 2012) https://www.cnet.com/news/microsoft-to-comply-with-eu-in-browser-choice-antitrust-probe/.

[85] Press Release, European Commission, *Antitrust: Commission fines Google €2.42 billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service* (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

[86] *See supra* note 81.

of superior design (in crafting relief by consent decree or injunction). In short, the Commission should articulate a philosophy of Permissionless Design, which we believe follows necessarily from the notion of Permissionless Innovation.

Our goal here is not to prevent the Commission from acting on legitimate cases, but merely to counsel humility in how the Commission proceeds. We have long called for the FTC to create a Bureau of Technology. (Indeed, one of us, Szóka, may have been the first to suggest this idea to Congress in Congressional testimony in 2012.[87]) A critical part of that Bureau, or any less formalized in-house expertise developed in the interim, must be expertise in product design. The Commission will need such expertise in the future, not merely to bring cases that need to be brought, but also to avoid making the mistakes of the European Commission's top-down approach to user interface design.

[87] Testimony of Berin Szóka, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?*, House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade at 16 (March 29, 2012), http://techfreedom.org/wp-content/uploads/2018/08/Szoka-Testimony-at-House-Balancing-Privacy-and-Innovation.pdf

The Federal Trade Commission:

Restoring Congressional Oversight of the Second National Legislature

AN ANALYSIS OF PROPOSED LEGISLATION

by Berin Szóka & Geoffrey A. Manne

May 2016

Report 2.0

FTC: Technology & Reform Project

The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature

AN ANALYSIS OF PROPOSED LEGISLATION

Berin Szóka[i] & Geoffrey A. Manne[ii]

May 2016

Report 2.0 of the FTC: Technology & Reform Project

The "FTC: Technology & Reform Project" was convened by the International Center for Law & Economics and TechFreedom in 2013. It is not affiliated in any way with the FTC.

Executive Summary

Congressional reauthorization of the FTC is long overdue. It has been twenty-two years since Congress last gave the FTC a significant course-correction and even that one, codifying the heart of the FTC's 1980 Unfairness Policy Statement, has not had the effect Congress expected. Indeed, neither that policy statement nor the 1983 Deception Policy Statement, nor the 2015 Unfair Methods of Competition Enforcement Policy Statement, will, on their own, ensure that the FTC strikes the right balance between over- and under-enforcement of its uniquely broad mandate under Section 5 of the FTC Act.

These statements are not without value, and we support codifying the other key provisions of the Unfairness Policy Statement that were not codified in 1980, as well as codifying the Deception Policy Statement. In particular, we urge Congress or the FTC to clarify the

[i] Berin Szóka is President of TechFreedom (techfreedom.org), a non-profit, tax-exempt think tank based in Washington D.C. He can be reached at bszoka@techfreedom.org or @BerinSzoka.

[ii] Geoffrey Manne is Executive Director of the International Center for Law & Economics (laweconcenter.org), a non-profit think tank based in Portland, Oregon. He can be reached at gmanne@laweconcenter.org or @GeoffManne.

meaning of "materiality," the key element of Deception, which the Commission has effectively nullified.

But a shoring up of substantive standards does not address the core problem: ultimately, that the FTC's *processes* have enabled it to operate with essentially unbounded discretion in developing the doctrine by which its three high level standards are applied in real-world cases.

Chiefly, the FTC has been able to circumvent judicial review through what it calls its "common law of consent decrees," and to effectively circumvent the rulemaking safeguards imposed by Congress in 1980 through a variety of forms of "soft law": guidance and recommendations that have, if indirectly and through amorphous forms of pressure, essentially regulatory effect.

At the same time, and contributing to the problem, the FTC has made insufficient use of its Bureau of Economics, which ought to be the agency's crown jewel: a dedicated, internal think tank of talented economists who can help steer the FTC's enforcement and policymaking functions. While BE has been well integrated into the Commission's antitrust decisionmaking, it has long resisted applying the lessons of law and economics to its consumer protection work.

The FTC is, in short, in need of a recalibration. In this paper we evaluate nine of the seventeen FTC reform bills proposed by members of the Commerce, Manufacturing and Trade Subcommittee, and suggest a number of our own, additional reforms for the agency.

Many of what we see as the most needed reforms go to the lack of economic analysis. Thus we offer detailed suggestions for how to operationalize a greater commitment to economic rigor in the agency's decision-making at all stages. Specifically, we propose expanding the proposed requirement for economic analysis of recommendations for "legislation or regulatory action" to include best practices (such as the FTC commonly recommends in reports), complaints and consent decrees. We also propose (and support bills proposing) other mechanisms aimed at injecting more rigor into the Commission's decisionmaking, particularly by limiting its use of various sources of informal or overly discretionary sources of authority.

The most underappreciated aspect of the FTC's processes is investigation, for it is here that the FTC wields incredible power to coerce companies into settling lawsuits rather than litigating them. Requiring that the staff satisfy a "preponderance of the evidence" standard for issuing consumer protection complaints would help, on the margin, to embolden some defendants not to settle. Other proposed limits on the aggressive use of remedies and on the allowable scope of the Commission's consent orders would help to accomplish the same thing. Changing this dynamic even slightly could produce a significant shift in the agency's model, by injecting more judicial review into the FTC's evolution of its doctrine.

Commissioners themselves could play a greater role in constraining the FTC's discretion, as well, keeping the FTC focused on advancing consumer welfare in everything it does. To-

gether with the Bureau of Economics, these two internal sources of constraint could partly substitute for the relative lack of external constraint from the courts.

We are not wholly critical of the FTC. Indeed, we are broadly supportive of its mission. And we support several measures to *expand* the FTC's jurisdiction to cover telecom common carriers and to make it easier for the FTC to prosecute non-profits that engage in for-profit activities. We enthusiastically support expansion of the FTC's Bureau of Economics. And we recommend expansion of the Commission's competition advocacy work into a full-fledged Bureau, so that the Commission can advocate at all levels of government — federal, state and local — on behalf of consumers and against legislation and regulations that would hamper the innovation and experimentation that fuel our rapidly evolving economy.

But most of all, Congress should not take the FTC's current processes for granted. Ultimately, the FTC reports to Congress and it is Congress's responsibility to regularly and carefully scrutinize how the agency operates. The agency's vague standards, sweeping jurisdiction, and its demonstrated ability to circumvent both judicial review and statutory safeguards on policy making make regular reassessment of the Commission through biennial reauthorization crucial to its ability to serve the consumers it is tasked with protecting.

Table of Contents

> Considering that rules of the Commission may apply to any act or practice "affecting commerce", and that the only statutory restraint is that it be unfair, **the apparent power of the Commission with respect to commercial law is virtually as broad as the Congress itself. In fact, the Federal Trade Commission may be the second most powerful legislature in the country….** All 50 State legislatures and State Supreme Courts can agree that a particular act is fair and lawful, but the five-man appointed FTC can overrule them all. **The Congress has little control over the far-flung activities of this agency short of passing entirely new legislation**.[1]
>
> *Sens. Barry Goldwater & Harrison Schmitt, 1980*

> **Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been "lawless" in the sense that it has traditionally been beyond judicial control**.[2]
>
> *Former FTC Chairman Tim Muris, 1981*

> **The FTC's investigatory power is very broad and is akin to an inquisitorial body.** On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[3]
>
> *Prof. Chris Hoofnagle, 2016*

Introduction

Only by the skin of its teeth did the Federal Trade Commission survive its cataclysmic confrontation with Congress in 1980. Today, the Federal Trade Commission remains the closest thing to a second national legislature in America. Its jurisdiction covers nearly every company in America. It powers over unfair and deceptive acts and practices (UDAP) and unfair methods of competition (UMC) remain so inherently vague that the Commission retains unparalleled discretion to make policy decisions that are essentially legislative. The Commission increasingly wields these powers over high tech issues affecting not just the high tech *sector*, but, increasingly, every company in America. It has become the de facto

---

[1] S. Rep. No. 96-184, at 18 (1980), *available at* http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=417102.

[2] Timothy J. Muris, *Judicial Constraints*, in THE FEDERAL TRADE COMMISSION SINCE 1970: ECONOMIC REGULATION AND BUREAUCRATIC BEHAVIOR, 35, 49 (Kenneth W. Clarkson & Timothy J. Muris, eds., 1981).

[3] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY 102 (2016).

Federal *Technology* Commission — a moniker we coined,[4] but which Chairwoman Edith Ramirez has embraced.[5]

For all this power, either by design or by neglect, the FTC is also "a largely unconstrained agency."[6] "Although appearing effective, most means of controlling Commission actions are virtually useless, owing to lack of political support and information, lack of interest on the part of those ostensibly monitoring the FTC, or FTC maneuvering."[7] At the same time, "[t]he courts place almost no restraint upon what commercial practices the FTC can proscribe…."[8]

The vast majority of what the FTC does is uncontroversial — routine antitrust, fraud and advertising cases. Yet, as the FTC has dealt with cutting-edge legal issues, like privacy, data security and product design, it has raised deep concerns not merely about the specific cases brought by the FTC, but also that the agency is drifting away from the careful balance it struck in its 1980 Unfairness Policy Statement (UPS)[9] and its 1983 Deception Policy Statement (DPS).[10]

We applaud the Commerce, Manufacturing & Trade Subcommittee for taking up the issue of FTC reform, and for the seventeen bills submitted by members of both parties. Even if no legislation passes this Congress, active engagement by Congress in the operation of the Commission was crucial in the past to ensuring that the FTC does not stray from its mission of serving consumers. But active congressional oversight has been wanting for far too long.

---

[4] Berin Szóka & Geoffrey Manne, *The Second Century of the Federal Trade Commission*, TECHDIRT (Sept. 26, 2013), *available at* https://www.techdirt.com/blog/innovation/articles/20130926/16542624670/second-century-federal-trade-commission.shtml*; see also Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission*, Report 1.0 of the FTC: Technology & Reform Project, 3 (Dec. 2013), *available at* http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[5] Kai Ryssdal, *The FTC is Dealing with More High Tech Issues*, MARKETPLACE (Mar. 7, 2016), *available at* http://www.marketplace.org/2016/03/07/tech/ftc-dealing-more-high-tech-issues.

[6] *Part I: The Institutional Setting*, in THE FEDERAL TRADE COMMISSION SINCE 1970, *supra* note 2 at 11.

[7] *Id*. at 11–12.

[8] Timothy J. Muris, *Judicial Constraints*, in *id*. 35, 43.

[9] *Letter from the FTC to the House Consumer Subcommittee, appended to* In re Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984) ["Unfairness Policy Statement" or "UPS"], *available at* http://www.ftc.gov/ftc-policy-statement-on-unfairness.

[10] *Letter from the FTC to the Committee on Energy & Commerce, appended to* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984) ["Deception Policy Statement" or "DPS"], *available at* http://www.ftc.gov/ftc-policy-statement-on-deception.

Not since 1996 has Congress reauthorized the FTC,[11] and not since 1994 has Congress actually substantially modified the FTC's standards or processes.[12]

The most significant thing Congress has done regarding the FTC since 1980 was the 1994 codification of the Unfairness Policy Statement's three-part balancing test in Section 5(n). But even that has proven relatively ineffective: The Commission pays lip service to this test, but there has been essentially none of analytical development promised by the Commission in the 1980 UPS:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, **subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time**.

The Commission no doubt believes that it has carefully weighed (1) substantial consumer injury with (2) countervailing benefit to consumers or to competition, and carefully assessed whether (3) consumers could "reasonably have avoided" the injury, as Congress required by enacting Section 5(n). But whatever weighing the Commission has done in its internal decision-making is far from apparent from the outside, and it has not been done by the courts in any meaningful way.[13] As former Chairman Tim Muris notes, "the Commission's authority remains extremely broad."[14]

The situation is little on better on Deception — at least, on the cutting edge of Deception cases, involving privacy policies, online help pages, and enforcement of other promises that differ fundamentally from traditional marketing claims. Just as the Commission has rendered the three-part Unfairness test essentially meaningless, it has essentially nullified the "materiality" requirement that it volunteered in the 1983 Deception Policy Statement. The Statement began by presuming, reasonably, that express *marketing* claims are always materi-

---

[11] Federal Trade Commission Reauthorization Act of 1996, Pub. L. 104-216, 110 Stat. 3019 (Oct. 1, 1996), *available at* http://uscode.house.gov/statutes/pl/104/216.pdf.

[12] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691 (Aug. 26, 1994) *available at* http://uscode.house.gov/statutes/pl/103/312.pdf.

[13] *See infra* at 39.

[14] Statement of Timothy J. Muris, Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation, 111th Cong. 2 (2010), 28, *available at* http://lawprofessors.typepad.com/files/muris_senate_testimony_ftc_role_protecting_consumers_3-17-101.pdf.

al, but the Commission has extended that presumption (and other narrow presumptions of materiality in the DPS) to cover essentially *all* deception cases.[15]

Congress cannot fix these problems simply by telling the FTC to dust off its two bedrock policy statements and take them more seriously (as it essentially did in 1994 regarding Unfairness). Instead, Congress must fundamentally reassess the *process* that has allowed the FTC to avoid judicial scrutiny of how it wields its discretion.

The last time Congress significantly reassessed the FTC's *processes* was in May 1980, when it created procedural safeguards and evidentiary requirements for FTC rulemaking. These reforms were much needed, and remain fundamentally necessary (although we do, below, encourage the FTC to attempt a Section 5 rulemaking for the first time in decades in order to provide a real-world experience of how such rulemakings work and whether Congress might make changes at the margins to facilitate reliance on that tool).[16]

But these 1980 reforms failed to envision that the Commission would, eventually, find ways of exercising the vast discretion inherent in Unfairness and Deception through what it now proudly calls its "common law of consent decrees"[17] — company-specific, but cookie-cutter consent decrees that have little to do with the facts of each case (and always run for twenty years). These consent decrees are bolstered by the regular issuance of recommended best practices in reports and guides that function as quasi-regulations, imposed on entire industries not by rulemaking but by the administrative equivalent of a leering glare. Together, these new tactics have allowed the FTC to effectively circumvent not only the process re-

---

[15] *See infra* at 21.

[16] *See infra* at 99.

[17] "Together, these enforcement efforts have established what some scholars call 'the common law of privacy' in the United States." Julie Brill, Commissioner, Fed. Trade Comm'n, *Remarks to the Mentor Group Forum for EU-US Legal-Economic Affairs Brussels, April 16, 2013*, 3 (Apr. 16, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-mentor-group-forum-eu-us-legal-economic-affairs-brussels-belgium/130416mentorgroup.pdf (citing Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States* (2010), *available at* http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8- 4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow.")). FTC Chairman Edith Ramirez said roughly the same thing in a 2014 speech:

> I have expressed concern about recent proposals to formulate guidance to try to codify our unfair methods principles for the first time in the Commission's 100 year history. While I don't object to guidance in theory, I am less interested in prescribing our future enforcement actions than in describing our broad enforcement principles revealed in our recent precedent.

Quoted in Geoffrey Manne, *FTC Commissioner Joshua Wright gets his competition enforcement guidelines*, TRUTH ON THE MARKET (Aug. 13, 2015), *available at* https://truthonthemarket.com/2015/08/13/ftc-commissioner-joshua-wright-gets-his-competiton-enforcement-guidelines/ (*speech video available at* http://masonlec.org/media-center/299).

forms of May 1980 but also the substantive constraints volunteered by the FTC later that year in the Unfairness Policy Statement and, three years later, in the Deception Policy Statement.

Such process reforms are the focus of this paper. The seventeen bills currently before the Subcommittee would begin to address these problems — but only begin. In this paper we evaluate nine of the proposed bills in turn, offer specific recommendations, and also offer a slate of our own additional suggestions for reform.

Our most important point, though, is not any one of our proposed reforms, but this: The default assumption should not be that the FTC continues operating indefinitely without course corrections from Congress.

Justice Scalia put this point best in his 2014 decision, striking down the EPA's attempt to "rewrite clear statutory terms to suit its own sense of how the statute should operate," when he said: "We are not willing to stand on the dock and wave goodbye as EPA embarks on this multiyear voyage of discovery."[18] The point is more, not less, important when a statute like Section 5 has been "deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion": trusting the FTC to follow an "evolutionary process" *requires* regular, searching reassessments by Congress. This need is especially acute given that the "underlying criteria" have *not* "evolve[d] and develop[ed] over time" through the "judicial review" expected by both Congress and the FTC in 1980 — at least, not in any analytically meaningful way.

Reauthorization should happen at regular two-year intervals and it should never be a *pro forma* rubber-stamping of the FTC's processes. Each reauthorization should begin from the assumption that the FTC is a uniquely important and valuable agency — one that can do enormous good for consumers, but also one whose uniquely broad scope and broad discretion require constant supervision and regular course corrections. Regular tweaks to the FTC's processes should be expected and welcomed, not resisted.

The worst thing defenders of the FTC could do would be allowing the FTC to drift along towards the kind of confrontation with Congress that nearly destroyed the FTC in 1980.

The FTC's History: Past is Prologue

It is no exaggeration to say that the 1980 compromise over unfairness saved the FTC from going the way of the Civil Aeronautics Board, which Congress began phasing out in 1978 under the leadership of Alfred Kahn, President Carter's de-regulator-in-chief. President

[18] Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2446 (2014).

Carter signed the 1980 FTC Improvements Act even though he objected to some of its provisions because, as he noted, "the very existence of this agency is at stake."[19] Those reforms to the FTC's rulemaking process, enacted in May 1980, were only part of what saved the FTC from oblivion.

Driven largely by outrage over the FTC's attempt to regulate children's advertising, Congress had allowed the FTC's funding to lapse, briefly shuttering the FTC. As Howard Beales, then (in 2004) director of the FTC's Bureau of Consumer Protection, noted, "shutting down a single agency because of disputes over policy decisions is almost unprecedented."[20] In the mid-to-late 1970s, the FTC had interpreted "unfairness" expansively in an attempt to regulate everything from funeral home practices to labor practices and pollution. Beales and former FTC Chairman, Tim Muris, summarize the problem thusly:

> Using its unfairness authority under Section 5, but unbounded by meaningful standards, in the 1970s the Commission embarked on a vast enterprise to transform entire industries. Over a 15-month period, the Commission issued a rule a month, usually without a clear theory of why there was a law violation, with only a tenuous connection between the perceived problem and the recommended remedy, and with, at best, a shaky empirical foundation.[21]

When the FTC attempted to ban the advertising of sugared cereals to children, the Washington Post dubbed the FTC the "National Nanny."[22] This led directly to the 1980 FTC Improvements Act — the one Sens. Goldwater and Schmitt endorsed in the quotation that opens this paper.

In early 1980, by a vote of 272-127, Congress curtailed the FTC's Section 5 rulemaking powers under the 1975 Magnuson-Moss Act, imposing additional evidentiary and procedural safeguards.[23] But the FTC refused to narrow its doctrinal interpretation of unfairness until Congress briefly shuttered the FTC in the first modern government shutdown. In December, 1980, the FTC issued its Unfairness Policy Statement, promising to weigh (a) sub-

---

[19] Jimmy Carter, *Federal Trade Commission Improvements Act of 1980 Statement on Signing H.R. 2313 into Law* (May 28, 1980), *available at* http://www.presidency.ucsb.edu/ws/?pid=44790.

[20] J. Howard Beales III, *Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present*, 8 n.32 (2004), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kids-and-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf.

[21] J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(B) of the FTC Act*, 79 ANTITRUST L. J. 1, 1 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764456.

[22] Editorial, WASH. POST (Mar. 1, 1978), reprinted in MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION, 69–70 (1982); *see also* Beales, *supra* note 20, at 8 n.37 ("Former FTC Chairman Pertschuk characterizes the Post editorial as a turning point in the Federal Trade Commission's fortunes.").

[23] Federal Trade Commission Act Improvements Act of 1980, Pub. L. 96-252, 94 Stat. 374 (May 28, 1980), *available at* http://uscode.house.gov/statutes/pl/96/252.pdf.

stantial injury against (b) countervailing benefit and (c) to focus only on practices consumers could not reasonably avoid. Last year, the FTC finally adopted a Policy Statement on Unfair Methods of Competition that parallels the two UDAP statements.[24]

In 1994, in Section 5(n), Congress codified the core requirements of the UPS, and further narrowed the FTC's ability to rely on its assertions of what constituted public policy. This was the last time Congress substantially modified the FTC Act — meaning that the Commission has operated since then without course-correction from Congress.[25] This is itself troubling, given that independent agencies are supposed to operate as creatures of Congress, not regulatory knights errant. But it is even more problematic given the extent of the FTC's renewed efforts to escape the bounds of even its minimal discretionary constraints.

The Inevitable Tendency Towards the Discretionary Model

To paraphrase Winston Churchill on democracy, the FTC offers the "worst form of consumer protection and competition regulation — except for all the others." Democracy, without constant vigilance and reform, will inevitably morph into the unaccountable exercise of power — what the Founders meant by the word "corruption" (literally, "decayed"). When Benjamin Franklin was asked, upon exiting the Constitutional Convention of 1787, "Well, Doctor, what have we got — a Republic or a Monarchy?," he famously remarked "A Republic, if you can keep it."[26]

The same can be said for the FTC: an "evolutionary process… subject to judicial review,"[27] *if we can keep it*. Any agency given so broad a charge as to prohibit "unfair methods of competition… and unfair or deceptive acts or practices…" will inevitably tend towards the exercise of maximum discretion.

This critique is of a dynamic inherent in the FTC itself, not of particular Chairmen, Commissioners, Bureau Directors or other staffers. The players change regularly, each leaving their mark on the agency, but the agency has institutional tendencies of its own, inherent in the nature of the agency.

The Commission itself most clearly identified the core of the FTC's institutional nature in the Unfairness Policy Statement, in a passage so critical it bears quoting in full:

---

[24] Fed. Trade Comm'n, *Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act* (Aug. 13, 2015) ["UMC Policy Statement"], *available at* https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

[25] The 1996 FTC reauthorization was purely *pro forma*.

[26] Benjamin Franklin, *quoted in* Respectfully Quoted: A Dictionary of Quotations, BARTLEBY.COM (last visited May 22, 2016), http://www.bartleby.com/73/1593.html

[27] UPS, *supra* note 9.

> The **present understanding of the unfairness standard is the result of an evolutionary process**. The **statute was deliberately framed in general terms** since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in **the expectation that the underlying criteria would evolve and develop over time**. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the **gradual process of judicial inclusion and exclusion**.'"[28]

In other words, Congress delegated vast discretion to the Commission from the very start because of the difficulties inherent in prescriptive regulation of competition and consumer protection. The Commission generally exercised that discretion primarily through case-by-case adjudication, but began issuing rules on its own authority in 1964,[29] setting it on the road that culminated in the cataclysm of 1980.

Indeed, given the essential nature of bureaucracies, it was probably only a matter of time before the FTC reached this point. It is no accident that it took just three years from 1975, when Congress affirmed the FTC's claims to "organic" rulemaking power (implicit in Section 5), until the FTC was being ridiculed as the "National Nanny." In short, the 1975 Magnuson-Moss Act created a monster, magnifying the effects of the FTC's inherent Section 5 discretion with the ability to conduct statutorily sanctioned rulemakings. If it had not been then-Chairman Michael Pertschuk who pushed the FTC too far, it probably would have, eventually, been some other chairman. The power was simply too great for any government agency to resist using without some feedback mechanism in the system telling it to stop.

In that sense, we believe the rise of the Internet played a role analogous to the 1975 Magnuson-Moss Act, spurring the FTC to greater activity where it had previously been more restrained.[30]

After 1980, the FTC ceased conducting new Section 5 rulemakings. Between 1980 and 2000, the FTC brought just sixteen unfairness cases, all of which fell into narrow categories of clearly "bad" conduct: "(1) theft and the facilitation thereof (clearly the leading category);

---

[28] UPS, *supra* note 9.

[29] Statement of Basis and Purpose, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (1964).

[30] Of course, we also recognize that other societal forces were at work, such as the Naderite consumer protection movement of the 1970s, and the growing privacy protection movement of the 1990s and 2000s. But the analogy still offers some value.

(2) breaking or causing the breaking of other laws; (3) using insufficient care; (4) interfering with the exercise of consumer rights; and (5) advertising that promotes unsafe practices."[31] Just how easy these cases were conveys in turn just how *cautious* the Commission was in using its unfairness powers — not only because it was chastened by the experience of 1980 but also because of Congress's reaffirmation of the limits on unfairness in its 1994 codification of Section 5(n). In a 2000 speech, Commissioner Leary summarized the Commission's restrained, "gap-filling" approach to unfairness enforcement over the preceding two decades:

> The overall impression left by this body of law is hardly that policy has been created from whole cloth. Rather, the Commission has sought through its unfairness authority to challenge commercial conduct that under any definition would be considered wrong but which escaped or evaded prosecution by other means.[32]

Yet even then Commissioner Leary noted his concerns about the burgeoning unfairness enforcement innovation in two of the Commission's then-recent cases: *Touch Tone* (1999)[33] and ReverseAuction (2000). Tellingly, his concern was over the Commission's failure to properly assess the substantiality of the amorphous privacy injuries alleged in those cases. Still, he concluded on a note of optimism:

> The extent of the disagreement should not be exaggerated, however. The majority [in *Reverse Auction*] did not suggest that all privacy infractions are sufficiently serious to be unfair and the minority did not suggest that none of them are. The boundaries of unfairness, as applied to Internet privacy violations, remain an open question.
>
> The Commission has so far used its unfairness authority in relatively few cases that involve the Internet. These cases, however, suggest that future application of unfairness will be entirely consistent with recent history. Internet technology is new, but we have addressed new technology before. I believe that the Commission will do what it can to prevent the Internet from becoming a lawless frontier, but it will also continue to avoid excesses of paternalism.
>
> The lessons of the past continue to be relevant because the basic patterns of dishonest behavior continue to be the same. Human beings evolve much more slowly than their artifacts.[34]

---

[31] Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1962 (2000).

[32] Thomas B. Leary, Former Commissioner of the Fed. Trade Comm'n, *Unfairness and the Internet*, II (Apr. 13, 2000), *available at* http://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

[33] *Id.* at II-C ("The unfairness count in Touch Tone also raised interesting questions about whether an invasion of privacy by itself meets the statutory requirement that unfairness cause "substantial injury." Unlike most unfairness prosecutions, there was no concrete monetary harm or obvious and immediate safety or health risks. The defendants' revenue came, not from defrauding consumers, but from the purchasers of the information who received exactly what they had requested.").

[34] *Id.*, at III-IV.

The Commission began bringing cases in 2000 alleging that companies employed unreasonable data security practices. While these early cases alleged that the practices were "unfair *and* deceptive," they were, in fact, pure deception cases.[35] In 2005, the FTC filed its first pure unfairness data security action, against BJ's Warehouse. Unlike past defendants, BJ's had, apparently, made no promise regarding data security upon which the FTC could have hung a deception action.[36] Since 2009, we believe the Commission has become considerably more aggressive in its prosecution of unfairness cases, not just about data security, but about privacy and other high tech issues like product design.

Yet it would be hard to pinpoint a single moment when the FTC's approach changed, or to draw a clear line between Republican data security cases and Democratic ones. And this is precisely a function of the first of the two crucial attributes of the modern FTC with which we are concerned: Legal doctrine continues to evolve even in the absence of judicial decisions, its evolution just becomes less transparent and more amorphous. As Commissioner Leary remarked in a footnote that now seems prescient:

> Because this case was settled, I cannot be sure that the other Commissioners agreed with this rationale.[37]

Indeed, this is the crucial difference between the FTC's pseudo common law and *real* common law. There is an observable directedness to the evolution of the real common law, which rests on a sort of ongoing conversation among the courts and the economic actors that appear before them. The FTC's ersatz common law, however, has little of this directedness or openness, and the conversations that do occur are more like whispered tête-à-têtes in the corner that someone else occasionally overhears.

But the second point is actually the more important, although the two are related: In this institutional structure, how often individual Commissioners dissent and how much rigor they demand matters far, far less than the structure of the agency itself. There is only so much an individual can do to divert the path of an already-steaming ship.

This leads back to the point made above: that we should expect regulatory agencies, over time, to expand their discretion as much as the constraints upon the agency allow. In this, regulatory agencies resemble gases, which, when unconstrained, do not occupy a fixed volume (defined by a clear statutory scheme, as in the Rulemaking Model) but rather expand to

---

[35] See, e.g., FTC v. Rennert, Complaint, FTC File No. 992 3245, http://www.ftc.gov/os/2000/07/iogcomp.htm (2000); In re Eli Lilly, Complaint, File No. 012 3214, http://www.ftc.gov/os/2002/05/elilillycmp.htm (2002).

[36] Complaint, In the Matter of BJ's Wholesale Club, Inc., a corporation, Fed. Trade Comm'n Docket No. C-4148, *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

[37] Leary, *Unfairness and the Internet*, *supra* note 32, n.50.

fill whatever space they occupy. What ultimately determines the size, volume and shape of a gas is its container. So, too, with regulatory agencies: what ultimately determines an agency's scale, scope, and agenda are the external constraints that operate upon it.

The FTC has evolved the way it has because, most fundamentally, Section 5 offers little in the way of prescriptive, statutory constraints, and because the FTC's processes have enabled it to operate case-by-case with relatively little meaningful, ongoing oversight from the courts.

We distinguish this from two other models of regulation: (1) the **Rulemaking Model**, in which the agency's discretion is constrained chiefly by the language of its organic statute, procedural rulemaking requirements and the courts; and (2) the **Evolutionary Model**, in which the agency applies a vague standard case by case, but is constrained in doing so by its ongoing interaction with the courts.[38] By contrast, we call the FTC's current approach the **Discretionary Model**, in which the agency also applies a vague standard case-by-case, but in which it operates without meaningful judicial oversight, such that doctrine evolves at the Commission's discretion and with little of the transparency provided by published judicial opinions. (Dialogue between majority and minority Commissioners seldom approaches the analysis of judicial opinions.)

We believe there is an inherent tendency of agencies that begin with an Evolutionary Model — which is very much the design of the FTC — to slide towards the Discretionary Model, simply because all agencies tend to maximize their own discretion, and because the freedom afforded by the lack of statutory constraints on substance or the agency's case-by-case process enable these agencies to further evade judicial constraints. The only way to check this process, without, of course, simply circumscribing its discretion by substantive statute (i.e., amending section 5(a)(2)), is regular assessment and course-correction by Congress — not with the aim of its own micromanagement of the agency, but rather with the aim of invigorating the ability of the courts to exert their essential role in steering doctrine.

This is not to be taken as an admission of defeat or a condemnation of the Commission. There is no reason to think that the FTC was in every way ideally constituted from the start (or in 1980 or in 1994), that its model could perform exactly as intended and perfectly in the public interest no matter what changed around it. Rather, limited, thoughtful oversight by

---

[38] We derive the term "evolutionary" from the Unfairness Policy Statement itself, *supra* note 9:

> *The present understanding of the unfairness standard is the result of an evolutionary process*. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time.

Congress is simply in the nature of the beast. As Justice Holmes said (of the importance of free speech):

> That, at any rate, is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year, if not every day, we have to wager our salvation upon some prophecy based upon imperfect knowledge.[39]

That, in a nutshell, is why regular reauthorization is critical for agencies like the FTC. As President Carter said, "[w]e need vigorous congressional oversight of regulatory agencies." This is more true for the FTC — with its vast discretion, immense investigative power, and all-encompassing scope — than any other agency. As we wrote in the precursor to this report:

> Thus, while the Congress of 1914 intended to create an agency better suited than itself to establish a flexible but predictable and consistent body of law governing commercial conduct, the modern trend of administrative law has relaxed the requirement that an agency's output be predictable or consistent.
>
> The FTC has embraced this flexibility as few other agencies have. Particularly in its efforts to keep pace with changing technology, the FTC has embraced its role as an administrative agency, and frequently sought to untether itself from ordinary principles of jurisprudence (let alone judicial review).[40]

The Doctrinal Pyramid

One of the chief reasons the FTC has come to operate the way it does is that the vocabulary around its operations is deeply confused, particularly around the word "guidance" and the term "common law." In an (admittedly first-cut) effort to introduce some concreteness, we view the various levels of "guidance" as steps in a Doctrinal Pyramid that looks something like the following, from highest to lowest degrees of authority:

1. **The Statute**: Section 5 (and other, issue-specific statutes)
2. **Litigated Cases**: Only these are technically binding on courts, thus they rank near the top of the pyramid, even though they are synthesized in, or cited by, the guidance summarized below. There are precious few of these on Unfairness or the key emerging issues of Deception
3. **Litigated Preliminary Injunctions**: Less meaningful than full adjudications of Section 5, these are, unfortunately, largely the only judicial opinions on Section 5.
4. **High-Level Policy Statements**: Unfairness, Deception, Unfair Methods of Competition

---

[39] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting).

[40] *Consumer Protection & Competition Regulation in a High-Tech World, supra*, note 4.

5. **Lower-Level Policy Statements**: The now-rescinded Disgorgement Policy Statement, the (not-yet existent) Materiality Statement we propose, *etc.*
6. **Guidelines**: Akin to the several DOJ/FTC Antitrust Guidelines, synthesizing past approaches to enforcement into discernible principles to guide future enforcement and compliance
7. **Consent Decrees**: Not binding upon the Commission and hinging (indirectly) upon the very low bar of whether the Commission has "reason to believe" a violation occurred, these provide little guidance as to how the FTC really understands Section 5
8. **Closing Letters**: Issued by the staff, these letters at times provide some limited guidance as to what the staff believe is *not* illegal
9. **Reports & Recommendations**: In their current form, the FTC's reports do little more than offer the majority's views of what companies should do to comply with Section 5, but carefully avoid any real legal analysis
10. **Industry Guides**: Issue-specific discussions issued by staff (*e.g.*, photo copier data security)
11. **Public Pronouncements**: Blog posts, press releases, congressional testimony, FAQs, etc.

In essence, under today's Discretionary Model, the FTC puts great weight on the base of the pyramid, while doing little to develop the top. Under the Evolutionary Model, the full Commission would develop doctrine primarily through litigation, and do everything it possibly could to provide guidance at higher levels of the pyramid, such as by debating, refining and voting upon new Policy Statements on each of the component elements of Unfairness and Deception and Guidelines akin to the Horizontal Merger Guidelines. Instead, the FTC staff issues Guides and other forms of casual guidance. Yet not all "guidance" is of equal value. Indeed, much of the "guidance" issued by the FTC serves not to constrain its discretion, but rather to expand it by increasing the agency's ability to coerce private parties into settlements — which begins the cycle anew.

Our Proposed Reforms

Seventeen bills have been introduced in the House Energy & Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade aimed at reforming the agency for the modern, technological age and improving FTC process and subject-matter scope in order to better protect consumers. Most of these will, we hope, be consolidated into a single FTC Reauthorization Act of 2016, passed in both chambers, and signed by the President.

With the hope of aiding this process, we describe and assess nine of these proposed bills, focusing in particular on whether and how well each proposal addresses the fundamental issues that define the problems of today's FTC. In broad strokes, the proposed bills address the following areas:

- Substantive standards
- Enforcement and guidance
- Remedies

- Other process issues
- Jurisdictional issues
- Other issues

Our analysis addresses the bills within the context of these broad categories, and adds our own suggestions (and one additional category: Competition Advocacy) for both minor amendments and additional legislation in each category.

Despite our concerns, we remain broadly supportive of the FTC's mission and we generally support expanding the agency's jurisdiction, to the extent that doing so effectively addresses substantial, identifiable consumer harms or reduces the scope of authority for sector-specific agencies. Although the process reforms proposed in these bills are, we believe, relatively minor, targeted adjustments, taken together they would do much to make the FTC more effective in its core mission of maximizing consumer welfare. But these proposed reforms are only a beginning.

Even if all of these reforms were enacted immediately, they would not fundamentally, or even substantially, change the core functioning of the FTC — and the core problem at the FTC today: its largely unconstrained discretion.

The FTC loudly proclaims the advantages of its *ex post* approach of relying on case-by-case enforcement of UDAP and UMC standards rather than rigid *ex ante* rulemaking, especially over cutting-edge issues of consumer protection. And there is much to commend this sort of approach relative to the prescriptive regulatory paradigm that characterizes many other agencies — again, the Evolutionary Model. But under the FTC's *Discretionary* Model, the Commission uses its "common law of consent decrees" (more than a hundred high-tech cases settled without adjudication, and with essentially zero litigated cases to guide these settlements) and a mix of other forms of soft law (increasingly prescriptive reports based on workshops tailored to produce predetermined outcomes, and various other public pronouncements), to "regulate" — or, more accurately, to try to steer — the evolution of technology.

The required balancing of tradeoffs inherent in unfairness and deception have little meaning if the courts do not review, follow or enforce them; if the Bureau of Economics has little role in the evaluation of these inherently economic considerations embodied in the enforcement decision-making of the Bureau of Consumer Protection or in its workshops; and if other Commissioners are able only to quibble on the margins about the decisions made by the FTC Chairman. Simply codifying these standards, as Congress codified the heart of the Unfairness Policy Statement in Section 45(n) back in 1994, and as the proposed CLEAR Act would finish doing, will not solve the problem: The FTC has routinely circumvented the rigorous analysis demanded by these standards, and the same processes would enable it to continue doing so.

To address these concerns, we also propose here a number of further process reforms that we believe would begin to correct these problems and ensure that the Commission's process really does serve the consumers the agency was tasked with protecting.

Our aim is not to hamstring the Commission, but to ensure that it wields its mighty powers with greater analytical rigor — something that should inure significantly to the benefit of consumers. Ideally, the impetus for such rigor would be provided by the courts, through careful weighing of the FTC's implementation of substantive standards in at least a small-but-significant percentage of cases. Those decisions would, in turn, shape the FTC's exercise of its discretion in the vast majority of cases that will — and should, in such an environment — inevitably settle out of court. The Bureau of Economics and the other Commissioners would also have far larger roles in ensuring that the FTC takes its standards seriously. But reaching these outcomes requires adjustment to the Commission's *processes*, not merely further codification of the standards the agency already purports to follow.

We believe that our reforms should attract wide bipartisan support, if properly understood, and that they would put the FTC on sound footing for its second century — one that will increasingly see the FTC assert itself as the Federal Technology Commission.

FTC Act Statutory Standards

Unfairness

The Statement on Unfairness Reinforcement & Emphasis (SURE) Act

Rep. Markwayne Mullin's (R-OK) bill (H.R. 5115)[41] further codifies promises the FTC made in its 1980 Unfairness Policy Statement — thus picking up where Congress left off in 1994, the last time Congress reauthorized the FTC in Section 5(n):

> The Commission shall have no authority … to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice [i] causes or is likely to cause substantial injury to consumers [ii] which is not reasonably avoidable by consumers themselves and [iii] not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[42]

[41] The Statement on Unfairness Reinforcement and Emphasis Act, H.R. 5115,114th Cong. (2016) [hereinafter SURE Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5115/text.

[42] 15 U.S.C. § 45(n).

This effectively codified the core of the Unfairness Policy Statement, while barring the FTC from relying on public policy determinations alone.[43] The bill would add several additional clauses to Section 5(n), drawn from the Unfairness Policy Statement. Most importantly:

1. It would exclude "trivial or merely speculative" harm from the definition of "substantial" injury.[44]
2. It would enhance the Act's "countervailing benefits" language to require consideration of the "net effects" of conduct, including dynamic, indirect consequences (like effects on innovation).[45]
3. It would prohibit the Commission from "second-guess[ing] the wisdom of particular consumer decisions," and encourage it to ensure "the free exercise of consumer decisionmaking."[46]

These provisions in particular (along with the others included in the bill, to be sure) would codify core aspects of the economic trade-off embodied in the UPS. They would enhance the Commission's administrative efficiency and direct its resources where consumers are most benefited. They would ensure that the FTC's weighing of costs and benefits is as comprehensive as possible, avoiding the systematic focus on concrete, short-term costs to the exclusion of larger, longer-term benefits. And they would help to preserve the inherent benefits of consumer choice, and avoid the intrinsic costs of agency paternalism.

Codification of these provisions would benefit consumers. And because H.R. 5115's language hews almost verbatim to the Unfairness Policy Statement, it should be uncontroversial. Effectively, it simply makes binding those parts of the UPS that Congress did not codify back in 1994.

---

[43] The Unfairness Policy Statement had said:

> Sometimes public policy will independently support a Commission action. This occurs when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission….
>
> To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values. The policy should likewise be one that is widely shared, and not the isolated decision of a single state or a single court. If these two tests are not met the policy cannot be considered as an "established" public policy for purposes of the S&H criterion. The Commission would then act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury.

UPS, *supra* note 9.

[44] SURE Act, *supra* note 41.

[45] *Id.*

[46] *Id.*

VALUE OF THE BILL: Codifying the Unfairness Policy Statement Would Reaffirm its Value, Encouraging Dissents and Litigation

Codifying a policy statement, even if verbatim and only in part, does essentially four things:

1. Legally, it makes the policy binding upon the Commission, since Policy Statements, technically, are not. On the margin this should deter the FTC from bringing more-tenuous cases that may not benefit consumers but that it might otherwise have brought.
2. Practically, it confers greater weight on the codified text in the Commission's deliberations, empowering dissenting Commissioners to point to the fact that Congress has chosen to codify certain language and requiring the majority to respond.
3. Legally, it somewhat reduces the deference the courts will give the FTC when it applies the statute (under *Chevron*) relative to the stronger deference given to agencies applying their own policy statements (under *Auer*).[47]
4. Perhaps most importantly, it gives defendants a stronger leg to stand on in court, thus increasing, on the margin, the number that will actually litigate rather than settle. That, in turn, benefits everyone by increasing the stock of judicial analysis of doctrine.

In all four respects, the FTC would greatly benefit from the H.R. 5115's further codification of the Unfairness Policy Statement. As a string of dissenting statements by former Commissioner Wright make lays bare, the FTC is not consistently taking the Unfairness Policy Statement seriously.[48] At most, it pays lip service even to the three core elements of unfairness set forth in Section 5(n) — and even less regard to those aspects of the UPS not codified in Section 5(n).[49]

Indeed, it is difficult to imagine any principled objection to codifying a document that the FTC already claims to observe carefully. And if the agency plans to bring unfairness cases that are *not* covered by the four corners of the Unfairness Policy Statement (yet somehow within Section 5(n)), that should be a matter of grave concern to Congress.

---

[47] Note that not everyone agrees that *Chevron* deference is weaker than *Auer* deference. *See* Sasha Volokh, *Auer and Chevron*, THE VOLOKH CONSPIRACY (Mar. 22, 2013), *available at* http://volokh.com/2013/03/22/auer-and-chevron/.

[48] *See, e.g.*, Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108 (Jan. 15, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf. *See also* Berin Szóka, *Josh Wright's Unfinished Legacy: Reforming FTC Consumer Protection Enforcement*, TRUTH ON THE MARKET (Aug. 26, 2015), https://truthonthemarket.com/2015/08/26/josh-wrights-unfinished-legacy/.

[49] UPS, *supra* note 9.

RECOMMENDATION: Require a Preponderance of the Evidence Standard for Unfairness Complaints

As valuable as codification of the substantive standards of the Unfairness Policy Statement would be, mere codification, or even tweaking, is unlikely to change much about the FTC's apparent evasion of its obligation to adhere to those standards. Rather, unless the *process* of enforcement by which the FTC has evaded the limits of the Statement is adjusted, the Commission will remain free to avoid the rigor it contemplates.

Indeed, it is far from clear that even the 1994 codification of the heart the Unfairness Policy Statement has been effective in actually changing the FTC's approach to enforcement. It is certainly possible that, but for Section 5(n), the Commission would have taken an even more aggressive approach to unfairness, and done even less to analyze its component elements in enforcement actions.

The process reforms we propose below are intended either (a) to increase the likelihood that the FTC will actually litigate unfairness cases, thus gaining judicial development of the doctrine, (b) that the Commissioners themselves will better develop doctrine through debate, or (c) that FTC staff, particularly through the involvement of the Bureau of Economics, will do so. Some combination of these (and, doubtless, other) reforms is essential to giving effect to Section 5(n) in its current form, to say nothing of expanding 5(n).

But the reform that would make the biggest difference within 5(n) itself would be to amend the existing Section 5(n) as follows:

> The Commission may not issue a complaint under this section unless the Commission demonstrates by a **preponderance of objective evidence** that an act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

The preponderance of the evidence standard is certainly a higher standard than the FTC currently faces for bringing complaints, but only because that standard is so absurdly low under Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[50] The "preponderance of the evidence" standard is the same standard used in civil cases, simply requiring that civil plaintiffs provide evidence that that their argument is "more likely than not" to get judgement against defendants. This standard is substantially less stringent than the "beyond a reasonable doubt" standard used in criminal cases, or the "clear and convincing" standard used in habeas petitions, so it should be suitable for the FTC's unfairness work.

---

[50] 15 U.S.C. § 45(b).

Why should the FTC have a higher burden (than it does today) at this intermediate stage in its enforcement process, when it brings a complaint? The FTC has significant pre-complaint powers of investigation at its disposal; it will have had considerable opportunity to perform discovery *before* bringing its complaint. Unlike private plaintiffs, who must first survive a *Twombly/Iqbal* motion to dismiss before they can compel discovery, typically at their own expense, the FTC can do so (through its civil investigative demand power) — and impose all of its costs on potential defendants — *before* ever alleging wrongdoing.

As we discuss in more detail below,[51] in order to justify the massive expense of this pre-complaint discovery process, it is not enough that it enables the Commission to engage in fishing expeditions to "uncover" possible violations of the law. Rather, if it is to be justified, and if its use by the Commission is to be kept consistent with its consumer-welfare mission, it must tend to lead to enforcement only when complaints can be justified by the weight of the evidence uncovered. A heightened burden is more likely to ensure this fealty to the consumer interest and to reduce the inefficient imposition of discovery costs on the wrong enforcement targets.

It is also important to note that, although we disagree strongly with their claims,[52] several FTC Commissioners and commentators have asserted that the set of consent orders entered into by the Commission with various enforcement targets constitute a *de facto* common law: "Technically, consent orders legally function as contracts rather than as binding precedent. Yet, in practice, the orders function much more broadly…."[53] In making these claims, proponents, including the Commission's current Chairwoman,[54] assert that "the trajectory and

---

[51] *See infra* at 31.

[52] *See, e.g.*, Berin Szóka, *Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection "Case Law,"* (2014 TPRC Conference Paper, Jul. 15, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418572; Geoffrey A. Manne & Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security*, *available at* http://masonlec.org/site/rte_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf.

[53] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 607 (2014).

[54] *Address by FTC Chairwoman Edith Ramirez,* at 6, at the Competition Law Center at George Washington University School of Law (Aug. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/735411/150813section5speech.pdf ("As I have emphasized, I favor a common law approach to the development of Section 5 doctrine."). The previous chairwoman held the same view. *See* Commissioner Julie Brill, *Privacy, Consumer Protection, and Competition*, speech given at 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-andcompetition/120427loyolasymposium.pdf ("Yet our privacy cases are also more generally informative about data collection and use practices that are acceptable, and those that cross the line, under Section 5 of the Federal Trade Commission Act creating what some have referred to as a common law of privacy in this country.").

development [of FTC enforcement] has followed a predictable set of patterns… [that amount to] the functional equivalent of common law."[55]

For these claims to be true or worthy, it would seem necessary, *at a minimum,* that the Commission's consumer protection complaints, which are virtually always coupled with consent orders upon their release (because *there is no statutory standard for settling FTC enforcement actions*), be tied to substantive standards that go beyond the mere exercise of three commissioners' discretion. And yet the FTC and the courts have consistently argued that the FTC Act's "reason to believe" standard for issuance of complaints requires nothing more than this minimal exercise of discretion. As former Commissioner Tom Rosch put it,

> [t]he "reason to believe" standard, however, is not a summary judgment standard: it is a standard that simply asks whether there is a reason to believe that litigation may lead to a finding of liability. That is a low threshold…. [T]he "reason to believe" standard is amorphous and can have an "I know it when I see it" feel."[56]

This creates a real problem for the claims that the Commission's consent orders have any kind of precedential power:

> In theory, the questions of whether to bring an enforcement action and whether a violation occurred are distinct; but in practice, when enforcement actions end in settlements (and when the two are often filed simultaneously), the two questions collapse into one. The FTC Act does not impose any additional requirement on the FTC to negotiate a settlement…. Thus, at best, the FTC's decisions are roughly analogous not to court decisions on the merits, but to court decisions on motions to dismiss…. Or, perhaps even more precisely, the FTC's decisions are analogous to reviews of warrants in criminal cases, as Commissioner Rosch has argued. It would be a strange criminal common law, indeed, that confused ultimate standards of guilt with the far lower standard of whether the police could properly open an investigation, yet this is essentially what the FTC's "common law" of settlements does.[57]

The incentives, discussed in more detail below,[58] that impel nearly every FTC consumer protection enforcement target to settle with the agency ensure that the only practical inflec-

---

[55] Solove & Hartzog, *supra* note 53, at 608.

[56] J. Thomas Rosch, Commissioner, Fed. Trade Comm'n, *Remarks at the American Bar Association Annual Meeting*, 3–4 (Aug. 5, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/so-i-serve-both-prosecutor-and-judge-whats-big-deal/100805abaspeech.pdf.

[57] Berin Szóka, *Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection "Case Law"* 7-8, available at http://masonlec.org/site/rte_uploads/files/Szoka%20for%20GMU%20FTC%20Workshop%20-%20May%202014.pdf.

[58] See *infra* at 31.

tion point at which the entire enforcement process is subject to any kind of "review," is when the Commissioners vote to authorize the issuance of a formal complaint and, simultaneously, approve an already-negotiated settlement. That such a determination may be based solely on the effectively unreviewable[59] discretion of the Commission that the complaint — not the consent order — meets the current, low threshold is troubling.

As former FTC Chairman Tim Muris observed, "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[60] If meaningful judicial review is ever to be brought to bear on the final agency decisions embodied in consent orders, it is crucial that the complaints that give rise to those settlements be subject to a more meaningful standard that imposes some evidentiary and logical burden on the Commission beyond the mere exercise of its discretion. While a preponderance of the evidence standard would hardly impose an insurmountable burden on the agency, it would at least impose a standard that is more than purely discretionary, and thus reviewable by courts and subject to recognizable standards upon which such review could proceed. Most importantly, enacting such a standard should, on the margin, embolden defendants to resist settling cases, thus producing more judicial decisions, which could in turn constrain the FTC's discretion.

None of our proposed reforms to the FTC's investigation process[61] would in any way undermine the FTC's ability to gather information prior to issuing a complaint. The FTC would still be able to contact parties and investigate them through its 6(b) powers and use civil investigative demands if necessary to compel disclosure. But it is necessary to heighten the FTC's standard for finally bringing a complaint since it can do significant investigation beforehand. It is not unreasonable to think they should have enough evidence to determine a violation of the law by a preponderance of the evidence by the point of complaint, especially since this is where most enforcement actions end in settlement.

Deception & Materiality

No Bill Proposed

The FTC's 1983 Deception Policy Statement forms one of the two pillars of its consumer protection work. As with Unfairness, the purpose of the Deception power is to protect consumers from injury. But unlike Unfairness, Deception does not require the FTC to prove injury. Instead, the FTC need prove only materiality — as an evidentiary proxy for injury:

---

[59] *See* FTC v. Standard Oil Co. of Cal., 449 U.S. 232 (1980).

[60] Muris, *supra* note 8, at 49.

[61] *See infra* at 31.

> [T]he representation, omission, or practice must be a "material" one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception. **In many instances, materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary**. Thus, the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment….[62]
>
> A finding of materiality is also a finding that injury is likely to exist because of the representation, omission, sales practice, or marketing technique. Injury to consumers can take many forms. **Injury exists if consumers would have chosen differently but for the deception**. **If different choices are likely, the claim is material, and injury is likely as well. Thus, injury and materiality are different names for the same concept**.[63]

Materiality is the *point* of the Deception Policy Statement. It is a shortcut by which the FTC can protect consumers from injury (*i.e.*, not getting the benefit of the bargain promised them) without having to establish injury (that failing to get this benefit actually harms them). A finding of materiality allows the FTC to presume injury because, in the traditional marketing context, a deceptive claim that is "material" enough to alter consumer behavior (which is the *point* of marketing, after all) may reasonably be presumed to do so in ways that a truthful claim wouldn't (or else why bother making the misleading claim?).

Unfortunately, the FTC has effectively broken the logic of the materiality "shortcut" by extending a *second* set of presumptions: most notably, that all express statements are material. This presumption may make sense in the context of traditional marketing claims, but it breaks down with things like privacy policies and other non-marketing claims (like online help pages) — situations where deceptive statements certainly *may* alter consumer behavior, but in which such an effect can't be presumed (because the company making the claim is not doing so in order to convince consumers to purchase the product).[64]

The FTC has justified this presumption-on-top-of-a-presumption by pointing to this passage of the DPS (shown with the critical footnotes):

---

[62] *DPS supra* note 10.

[63] *Id.* at 6 (emphasis added).

[64] Of course, even in the marketing context this presumption is one of administrative economy, not descriptive reality. While there is surely a correlation between statements intended to change consumer behavior and actual changes in consumer behavior, a causal assumption is not warranted. *See generally* Geoffrey A. Manne & E. Marcellus Williamson, *Hot Docs vs. Cold Economics: The Use and Misuse of Business Documents in Antitrust Enforcement and Adjudication*, 47 ARIZ. L. REV. 609 (2005).

> The Commission considers certain categories of information presumptively material.[47] First, the Commission presumes that express claims are material.[48] As the Supreme Court stated recently [in *Central Hudson Gas & Electric Co. v. PSC*], "[i]n the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising."
>
> [47] The Commission will always consider relevant and competent evidence offered to rebut presumptions of materiality.
>
> [48] Because this presumption is absent for some implied claims, the Commission will take special caution to ensure materiality exists in such cases.[65]

In effect, the first two sentences have come to swallow the rest of the paragraph, including the logic of the Supreme Court's decision in *Central Hudson,* the single most important case of all time regarding the regulation of commercial speech.[66] In particular, the FTC ignores the "absence of factors that would distort the decision to advertise."[67]

When the Deception Policy Statement talked about "express claims," it was obviously contemplating *marketing* claims, where the presumption of materiality makes sense: if a company buys an ad, anything it says in the ad is intended to convince the viewer to buy the product. The intention to advertise the product is simply the flipside of materiality — a way of inferring what reasonable buyers would think from what profit-maximizing sellers obviously intended. But this logic breaks down once we move beyond advertising claims.

We have written at length about this problem in the context of the FTC's 2015 settlement with Nomi, the maker of a technology that allowed stores to track users' movement on their premises, as well as a shopper's repeat visits, in order to deliver a better in-store shopping experience, placement of products, etc.[68]

The FTC's complaint focused on a claim made in the privacy policy on Nomi's website that consumers could opt out on the website or at "any retailer using Nomi's technology." Nomi failed to provide an in-store mechanism for allowing consumers to opt out of the tracking program, but it did provide one on the website — right where the allegedly deceptive claim was made. That Nomi did not, in fact, offer an in-store opt-out mechanism in violation of its express promise to do so is clear. Whether, taken in context, that failure was *material*, however, is not clear.

---

[65] *Id.* at 5.

[66] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of NY, 447 U.S. 557 (1980).

[67] *Id.* at 567–68.

[68] *See* Geoffrey A. Manne, R. Ben Sperry & Berin Szóka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case* (ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1), *available at* http://laweconcenter.org/images/articles/icle-nomi_white_paper.pdf.

For the FTC majority, even though the website portion of the promise was fulfilled, Nomi's failure to comply with the in-store portion amounted to an actionable deception. But the majority dodged the key question: whether the evidence that Nomi accurately promised a website opt-out, and that consumers could (and did) opt-out using the website, rebuts the presumption that the inaccurate, in-store opt-out portion of the statement was material, and sufficient to render the statement *as a whole* deceptive.

In other words, the majority assumed that Nomi's express claim, in the context of a privacy policy rather than a marketing statement, affected consumers' behavior. But given the very different purposes of a privacy policy and a marketing statement (and the immediate availability of the website opt-out in the very place that the claim was made), that presumption seems inappropriate. The majority did not discuss the reasonableness of the presumption given the different contexts, which *should* have been the primary issue. Instead it simply relied on a literal reading of the DPS, neglecting to consider whether its underlying logic merited a different approach.

The Commission failed to demonstrate that, *as a whole*, Nomi's failure to provide in-store opt out was deceptive, in clear contravention of the Deception Policy Statement's requirement that all statements be evaluated in context:

> [T]he Commission will evaluate the entire advertisement, transaction, or course of dealing in determining how reasonable consumers are likely to respond. Thus, in advertising the Commission will examine "the entire mosaic, rather than each tile separately."[69]

Moreover, despite the promise in the DPS that the Commission would "always consider relevant and competent evidence offered to rebut presumptions of materiality," the FTC failed to do so in *Nomi*. As Commissioner Wright noted in his dissent:

> [T]he Commission failed to discharge its commitment to duly consider relevant and competent evidence that squarely rebuts the presumption that Nomi's failure to implement an additional, retail-level opt out was material to consumers. In other words, the Commission neglects to take into account evidence demonstrating consumers would not "have chosen differently" but for the allegedly deceptive representation.
>
> Nomi represented that consumers could opt out on its website as well as in the store where the Listen service was being utilized. Nomi did offer a fully functional and operational global opt out from the Listen service on its website. Thus, the only remaining potential issue is whether Nomi's failure to offer the represented in-store opt out renders the statement in its privacy policy deceptive. The evi-

[69] *DPS supra* note 10, at 4 n.31 (quoting Fed. Trade Comm'n v. Sterling Drug, 317 F.2d 669, 674 (2d Cir. 1963)).

> dence strongly implies that specific representation was not material and therefore not deceptive. Nomi's "tracking" of users was widely publicized in a story that appeared on the front page of The New York Times, a publication with a daily reach of nearly 1.9 million readers. Most likely due to this publicity, Nomi's website received 3,840 unique visitors during the relevant timeframe and received 146 opt outs — an opt-out rate of 3.8% of site visitors. This opt-out rate is significantly higher than the opt-out rate for other online activities. This high rate, relative to website visitors, likely reflects the ease of a mechanism that was immediately and quickly available to consumers at the time they may have been reading the privacy policy.
>
> The Commission's reliance upon a presumption of materiality as to the additional representation of the availability of an in-store opt out is dubious in light of evidence of the opt-out rate for the webpage mechanism. Actual evidence of consumer behavior indicates that consumers that were interested in opting out of the Listen service took their first opportunity to do so. To presume the materiality of a representation in a privacy policy concerning the availability of an additional, in-store opt-out mechanism requires one to accept the proposition that the privacy-sensitive consumer would be more likely to bypass the easier and immediate route (the online opt out) in favor of waiting until she had the opportunity to opt out in a physical location. Here, we can easily dispense with shortcut presumptions meant to aid the analysis of consumer harm rather than substitute for it. The data allow us to know with an acceptable level of precision how many consumers — 3.8% of them — reached the privacy policy, read it, and made the decision to opt out when presented with that immediate choice. The Commission's complaint instead adopts an approach that places legal form over substance, is inconsistent with the available data, and defies common sense.[70]

The First Circuit's recent opinion in *Fanning v. FTC* compounds the FTC's error. First, it holds (we believe erroneously) that the DPS's presumptions aren't limited to the marketing milieu:

> There is no requirement that a misrepresentation be contained in an advertisement. The FTC Act prohibits 'deceptive acts or practices,' and we have upheld the Commission when it imposed liability based on misstatements not contained in advertisements.[71]

In addition, the *Fanning* decision would allow the FTC to go even a step further. Citing the language from the Deception Policy Statement that "claims pertaining to a central charac-

---

[70] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Nomi Technologies, Inc., at 3-4 (Apr. 23, 2015) (emphasis added), *available at* https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

[71] Fanning v. Fed. Trade Comm'n, No. 15-1520, slip op. at 13 (May 9, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/051816jerkopinion.pdf (citing *Sunshine Art Studios, Inc. v. FTC*, 481 F.2d 1171, 1173-74 (1st Cir. 1973) (finding FTC Act violation based on company's practice of sending customers excess merchandise and using "a fictitious collection agency to coerce payment")).

teristic of the product about 'which reasonable consumers would be concerned,'" are material, the First Circuit shifted the burden of proof to Fanning to prove that its promises were *not* material.

Of course, the DPS strongly suggests that this "central characteristic" language is also applicable only in the marketing context — in the context, that is, of claims made about a product's "central characteristics" in the service of *selling* that product — and that it is fact-dependent:

> Depending on the facts, information pertaining to the central characteristics of the product or service will be presumed material. Information has been found material where it concerns the purpose, safety, efficacy, or cost, of the product or service. Information is also likely to be material if it concerns durability, performance, warranties or quality.[72]

Much like *Nomi*, the effect of the First Circuit's decision could be far-reaching. If the FTC may simply assert that claims relate to the central characteristic of a product, receive a presumption of materiality on that basis, and then shift the burden the defendant to adduce evidence to the contrary, it may *never* need to offer any evidence of its own on materiality. Combined this with the reluctance of the FTC to actually consider evidence rebutting the presumption (as illustrated in *Nomi*), we could see cases where the FTC presumes materiality on the basis of mere allegation and ignores all evidence to the contrary offered in rebuttal, despite its promise to "always consider relevant and competent evidence offered to rebut presumptions of materiality.[73] This would lead to an outcome that the drafters of the Deception Policy Statement plainly did not intend: that effectively every erroneous or inaccurate word ever publicly disseminated by companies may be presumed to injure consumers and constitute an actionable violation of Section 5.

In short, if the courts will defer to the FTC even as it reads the materiality requirement out of the Deception Policy Statement, this is not a vindication of the FTC's reading; it is merely a reminder of the vastness of the deference paid to agencies in interpreting ambiguous statutes. And it should be a reminder to Congress that only through legislation can Congress ultimately reassert itself — if only to keep the FTC on the path the agency itself laid out decades ago.

RECOMMENDATION: Codify the 1983 Deception Policy Statement

Congress should codify the Deception Policy Statement in a new Section 5(o), just as it codified the core part of the Unfairness Policy Statement in 1994, and just as the SURE Act would codify the rest of the UPS today. Fully codifying both statements (all *three* statements,

---

[72] *DPS supra* note 10, at 5.

[73] *Id.* at n.47.

including the UMC Enforcement Policy Statement) is a good idea if only because the FTC is somewhat more likely to take them seriously if they are statutory mandates. But, as we have emphasized, codification alone will not do much to change the institutional structures and processes that are at the heart of the statements' relative ineffectiveness in guiding the FTC's discretion.

In codifying the DPS, Congress should be mindful of the problems we discuss above. It should also modify the DPS' operative language to mitigate the interpretative problems arising from its inevitable ambiguity. Without specifying precise language here, a few guidelines for drafting such language come readily to mind:

1. Defer to the DPS drafters: they could never have meant for the exceptions (presumptions) to subsume the rule (the materiality requirement), and the codified language should endeavor to reflect this.
2. Acknowledge that there are differences between marketing language and language used in other contexts, including, importantly, today's ubiquitous privacy policies and website terms of use — settings that weren't contemplated by the DPS drafters.
3. Clarify what evidentiary burden is required to demonstrate materiality in contexts where it shouldn't simply be inferred, and, after *Fanning*, clarify whether, and when, the burden should shift from the FTC to defendants.

RECOMMENDATION: Clarify that Legally Required Statements Cannot Be Presumptively Material

Particularly given the increasing importance of privacy policies in the FTC's deception enforcement practice, it is also important to clarify whether legally mandated language should be presumed material. We believe that the DPS' exception for "factors that would distort the decision to advertise" includes a legal mandate to say something, which unequivocally "distorts" the decision to proffer such language. Thus, in most cases, privacy policies — required by California law[74] — ought not be treated as presumptively material. This would not preclude the FTC from proving that they *are* material, of course. It would simply require the Commission to *establish* their materiality in each particular case — which, again, was the point of the Deception Policy Statement in the first place.

RECOMMENDATION: Delegate Reconsideration of Other Materiality Presumptions

Unfortunately, it will be difficult for Congress to address the other aspects of the FTC's interpretation of materiality by statute, because each is highly fact-specific. But, ultimately, ensuring that the FTC's implementation of the Deception Policy Statement's requirement of

[74] *See* CAL. BUS. & PROF. § 22575, *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579.

a rigorous assessment of trade-offs doesn't require specification of outcomes; it requires some institutional rejiggering ensure that the Bureau of Consumer Protection is motivated to do so by some combination of the courts, the commissioners, and the Bureau of Economics.

Instead of trying to address these issues directly, Congress could, for example, direct the FTC to produce a Policy Statement on Materiality in which the Commission attempts to clarify these issues on its own. Thus, for example, the Commission could describe factors for determining whether and when an online help center should be considered a form of marketing that merits the presumption. Or, as we have previously proposed, Congress could delegate this and other key doctrinal questions to a Modernization Commission focused on high-tech consumer protection issues like privacy and data security, parallel to the Antitrust Modernization Commission.[75]

RECOMMENDATION: Require Preponderance of the Evidence in Deception Cases

Above, we explain that among our top three priorities for additional reforms — indeed, for reforms overall — is adding a "preponderance of the evidence" standard for unfairness cases by expanding upon Section 5(n).[76] We urge Congress to include the same standard in a new Section 5(o) for non-fraud deception cases. Again, this standard should be easy for the FTC to satisfy.

Unfair Methods of Competition

No Bill Proposed

The Commission's unanimous adoption last year of a "Statement of Enforcement Principles Regarding 'Unfair Methods of Competition'" was a watershed moment for the agency.[77] The adoption of the Statement marked the first time in the Commission's 100-year history

---

[75] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf ("A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.").

[76] *See supra* note 18.

[77] Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

that the FTC issued enforcement guidelines for cases brought under the Unfair Methods of Competition ("UMC") provisions of Section 5 of the FTC Act.[78]

Enforcement principles for UMC actions were in desperate need of clarification at the time of the Statement's adoption. Without any UMC standards, the FTC had been essentially completely free to leverage its costly adjudication process into settlements (or short-term victories), and to leave businesses in the dark as to what sorts of conduct might trigger enforcement. Through a series of un-adjudicated settlements, UMC unfairness doctrine (such as it is) has remained largely within the province of FTC discretion and without judicial oversight. As a result, and either by design or by accident, UMC never developed a body of law encompassing well-defined goals or principles like antitrust's consumer-welfare standard. Several important cases had seemingly sought to take advantage of the absence of meaningful judicial constraints on UMC enforcement actions to bring standard antitrust cases under the provision.[79] And more than one recent Commissioner had explicitly extolled the virtue of the unfettered (and unprincipled) enforcement of antitrust cases the provision afforded the agency.[80] The new Statement makes it official FTC policy to reject this harmful dynamic.

The UMC Statement is deceptively simple in its framing:

> In deciding whether to challenge an act or practice as an unfair method of competition in violation of Section 5 on a standalone basis, the Commission adheres to the following principles:
>
> - the Commission will be guided by the public policy underlying the antitrust laws, namely, the promotion of consumer welfare;
> - the act or practice will be evaluated under a framework similar to the rule of reason, that is, an act or practice challenged by the Commission must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications; and

---

[78] It should be noted that the Statement represents a landmark victory for Commissioner Joshua Wright, who has been a tireless advocate for defining the scope of the Commission's UMC authority since before his appointment to the FTC in 2013. *See, e.g.*, Joshua D. Wright, *Abandoning Antitrust's Chicago Obsession: The Case for Evidence-Based Antitrust*, 78 ANTITRUST L. J. 241 (2012).

[79] For a succinct evaluation of these cases (including, e.g., *Intel* and *N-Data*), see Geoffrey A. Manne & Berin Szóka, *Section 5 of the FTC Act and monopolization cases: A brief primer*, TRUTH ON THE MARKET (Nov. 26, 2012), https://truthonthemarket.com/2012/11/26/section-5-of-the-ftc-act-and-monopolization-cases-a-brief-primer/.

[80] *See, e.g.*, Statement of Chairman Leibowitz and Commissioner Rosch, In the Matter of Intel Corp., Docket No. 9341, 1, *available at* https://www.ftc.gov/system/files/documents/public_statements/568601/091216intelchairstatement.pdf ("[I]t is more important than ever that the Commission actively consider whether it may be appropriate to exercise its full Congressional authority under Section 5.").

- the Commission is less likely to challenge an act or practice as an unfair method of competition on a standalone basis if enforcement of the Sherman or Clayton Act is sufficient to address the competitive harm arising from the act or practice.[81]

Most importantly, the Statement espouses a preference for enforcement under the antitrust laws over UMC when both might apply, and brings the weight of consumer-welfare-oriented antitrust law and economics to bear on such cases.

RECOMMENDATION: Codify the Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under a New Section 5(p) of the FTC Act

As beneficial as the Statement is, it necessarily reflects compromise. In particular, the third prong is expressed merely as a *preference* for antitrust enforcement rather than an obligation. And, of course, such statements are not binding on the Commission, no matter how strongly worded they may be, and no matter how much "soft law" may be brought to bear on the Commissioners charged with following it.

For these reasons, Congress should codify the most important aspects of the Statement — much as it did with the Unfairness Policy Statement's consumer-injury unfairness test — by adding the following language in a new Section 5(p):

> The Commission ***shall not*** challenge an act or practice as an unfair method of competition on a standalone basis if the alleged competitive harm arising from the act or practice is subject to enforcement under the Sherman or Clayton Act.
>
> An act or practice challenged by the Commission as an unfair method of competition must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications.

This language is taken directly from the UMC Statement, with the small tweak highlighted above *requiring* application of the antitrust laws instead of UMC in appropriate cases, rather than merely expressing a preference for doing so.

Such language would harmonize enforcement of all anticompetitive practices under the antitrust laws' consumer-welfare standard, while still permitting the few cases not amenable to Sherman or Clayton Act jurisdiction (*e.g.*, invitations to collude) to be brought by the Commission. Importantly, language such as this, which would make enforcement under the antitrust laws *obligatory* where both UMC and antitrust could apply, would transform the Statement's expression of agency preference into an enforceable statutory requirement.

---

[81] Statement of UMC Enforcement Principles, *supra* note 77.

Enforcement & Guidance

The FTC is commonly labeled a "law enforcement agency," but in reality it is an administrative agency that regulates primarily through enforcement rather than rulemaking:

> As an administrative agency, the FTC's primary form of regulation involves administrative application of a set of general principles — a "law enforcement" style function that, practically speaking, operates as administrative regulation….[82]

This administrative enforcement model puts significant emphasis on the agency's investigative power, and it is the investigatory aspect of its enforcement process that has become the agency's most powerful — and least overseen — tool. As one commentator notes, "[t]he FTC possesses what are probably the broadest investigatory powers of any federal regulatory agency."[83]

The Commission's investigatory process is also the heart of the mechanism by which the agency largely bypasses judicial oversight:

> [Not even] the courts have… been a significant factor in deterring FTC investigation. Indeed, the bulk of court cases appear to affirm the agency's authority to obtain information pursuant to the Federal Trade Commission Act. Thus, any constraints placed upon the FTC's ability to obtain information must lie elsewhere.[84]

By overly compelling companies to settle enforcement actions when they are little more than investigations, the investigative process inevitably leads, on the margin, to less-well-targeted investigations, increased discovery burdens on (even blameless) potential defendants, inefficiently large compliance expenditures throughout the economy, under-experimentation and innovation by firms, doctrinally questionable consent orders, and a relative scarcity of judicial review of Commission enforcement decisions.

More than any other aspect of the FTC Act or the FTC's operations, it is here that reinvigorated congressional oversight is needed. Even Chris Hoofnagle, who has long advocated that the FTC be far more aggressive on privacy and data security, warns, in his new treatise on privacy regulation at the agency, that

---

[82] *Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission*, *supra* note 4, at 12.

[83] Stephanie W. Kanwit, 1 Federal Trade Commission § 13:1 at 13-1 (West 2003).

[84] Darren Bush, *The Incentive and Ability of the Federal Trade Commission to Investigate Real Estate Markets: An Exercise in Political Economy*, 20-21, *available at* http://www.antitrustinstitute.org/files/517c.pdf.

> the FTC's investigatory power is very broad and is akin to an inquisitorial body. On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[85]

In competition cases, the entire Commission must vote to authorize CIDs in each matter and also vote to close investigations once compulsory process is issued. But in the consumer protection context, the Commission issues standing orders — "omnibus resolutions" (ORs) — authorizing extremely broad, industry-wide investigations that authorize the subsequent issuance of CIDs with the consent of only a single Commissioner. For instance, there is a standing Commission order authorizing staff to investigate telemarketing fraud cases.[86] Thus, if staff wants to issue a CID to investigate a specific telemarketer or any of a wide range of companies that may be supporting telemarketers, it need seek approval for the CID from only a single Commissioner. These requests are frequent (to the best of our knowledge amounting to many dozens *per week*), and routinely granted.

The staff's ability to rely upon Omnibus Resolutions in this manner bypasses an important aspect of how the FTC's enforcement approach is structured on paper. The FTC Operating Manual draws a clear line between initial phase investigations (initiated and run by the staff at their own discretion for up to 100 hours in consumer protection cases) and full investigations. The decision to upgrade an investigation can be made by the Bureau Director on delegated authority, but at least this creates some potential for involvement of other Commissioners. It also requires written analysis by the staff[87] — something other Commissioners could ask to see. But most relevant to the immediate discussion is the Commission's policy that

> Compulsory procedures are not ordinarily utilized in the initial phase of investigations; therefore, facts and data which cannot be obtained from existing sources must be developed through the use of voluntary procedures.[88]

Relying on ORs, however, the staff may make use of compulsory process even when it would not otherwise be appropriate to do so.

At the same time, the Commission may (if it so chooses) bring its Section 5 cases (those relatively few that don't settle) in its own administrative tribunal, whose decisions are appealed to the Commission itself. Only after the Commission's review (or denial of review) may a

---

[85] HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY, *supra* note 3, at 102.

[86] Resolution No. 0123145, "Resolution Directing the Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, and Others" Technically the Telemarketing Resolution expired in April 2016. But it authorizes continuing investigation subject to already-issued CIDs as long as necessary. Although no further CIDs will be issued, the investigation continues.

[87] Federal Trade Commission, *Operating Manual*, 3.5.1.2 [hereinafter Operating Manual].

[88] *Id.* at 3.2.3.2.

party bring its case before an Article III court. Needless to say, this adds an extremely costly layer of administrative process to enforcement, as former Commissioner Wright explains:

> [T]he key to understanding the threat of Section 5 is the interaction between its lack of boundaries and the FTC's administrative process advantages.... Consider the following empirical observation that demonstrates at the very least that the institutional framework that has evolved around the application of Section 5 cases in administrative adjudication is quite different than that faced by Article III judges in federal court in the United States. The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, **in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed**. By way of contrast, when the antitrust decisions of federal district court judges are appealed to the federal courts of appeal, plaintiffs do not come anywhere close to a 100 percent success rate. Indeed, the win rate is much closer to 50 percent.[89]

The net effect of these procedural circumstances is stark. Wright continues:

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may not [violate any law or regulation]. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's [Section 5] authority by **encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority**.[90]

Further, the Commission currently enjoys a nearly insurmountable presumption that its omnibus resolutions are proper — a fact that places subjects of investigations at a severe disadvantage when trying to challenge the Commission's often intrusive investigative process.

Whether issued under an Omnibus Resolution or otherwise, the Commission's CIDs allow the agency to impose enormous costs on potential defendants before even a single Commis-

---

[89] Joshua Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, CPI ANTITRUST CHRONICLE (Nov. 2013 (2)), at 4 (emphasis added), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf.

[90] *Id.* at 5 (emphasis added).

sioner — let alone the entire Commission or a court of law — determines that there is even a "reason to believe" that the party being investigated has violated any law.

The direct costs of compliance with these extremely broad CIDs can be enormous. Unlike discovery requests in private litigation, reimbursement of costs associated with CID compliance is not available, even if a defendant prevails. Among other things, CID recipients will be required to incur the expense of performing electronic and offline searches for copious amounts of information (which may require the hiring of outside vendors), interviewing employees, the business costs of lost employee and management time, and attorneys' fees. Moreover, there may be several CIDs issued to a single company. And, sometimes of greatest importance, in many cases publicly traded companies will be required to disclose receipt of a CID in its SEC filings. This can have significant immediate effects on a company's share price and do lasting damage to its reputation among consumers.

The experience of Wyndham Hotels is illustrative. The company became the first to challenge an FTC data security enforcement action following more than twelve years of FTC data security settlements. Even before it finally had recourse to an Article III court, Wyndham had already incurred enormous costs, as we noted in our amicus brief in support of Wyndham's 2013 motion to dismiss:

> Burdensome as settlements can be, *not* settling can be even costlier. Wyndham, for example, has already received 47 document requests in this case and spent $5 million responding to these requests. The FTC's compulsory investigative discovery process and administrative litigation both consume the most valuable resource of any firm: the time and attention of management and key personnel.[91]

And it is difficult for CID recipients to challenge a CID on the basis of cost. As the Commission notes in a ruling denying one such request:

> WAM [West Asset Management] has not satisfied its burden of demonstrating compliance with the CID would be unduly burdensome…. WAM has not cited, and the Commission is unaware of, any cases to support WAM's minimize-disruption standard. "Thus courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business." As in *Texaco* the breadth of the CID is a reflection of the comprehensiveness of the inquiry being undertaken and the magnitude of WAM's business operations.[92]

---

[91] Amici Curiae Brief Of TechFreedom, International Center for Law and Economics & Consumer Protection Scholars, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 2:13-cv-01887 (3d Cir. 2013) at 13.

[92] Request for Review of Denial of Petition to Limit Civil Investigative Demand, File No. 0723006 (Jul. 2, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/west-asset-management-inc./080702westasset.pdf (citing Fed. Trade Comm'n v. Texaco, Inc., 555 F.2d 862, 882 (D.C. Cir. 1977)).

High costs, as long as they don't threaten a company's viability, will be insufficient to quash or even minimize the scope of a CID. But even expenses that don't threaten viability can be extremely large and extremely burdensome. And, of course, broader costs (*e.g.*, on stock price and market reputation) are extremely difficult to measure and unaccounted for in the FTC's assessment of a CID's burden.

It should be noted that, unlike complaints (before adjudication) and consent orders, CIDs are directly reviewed by courts at times. For better or worse, however, courts are prone to give the Commission an extreme degree of deference when reviewing CIDs. "The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one… The requested material, therefore, need only be relevant to the investigation — the boundary of which may be defined quite generally."[93] Thus, the Commission has "'extreme breadth' in conducting … investigations."[94]

But high *direct* costs aren't even the most troubling part. The indirect, societal cost of overly broad CIDs is the increased propensity of companies to settle to avoid them. For reasons we also discuss elsewhere, an excessive tendency toward settlements imposes costs throughout the economy. Among other things:

- It reduces the salutary influence of judicial review of agency enforcement actions;
- It reduces the stock of judicial decisions from which companies, courts and the FTC would otherwise receive essential guidance regarding appropriate enforcement theories and the propriety of ambiguous conduct;
- It induces companies that haven't violated the statute to be saddled with remedies nonetheless, and thereby induces other, similarly-situated companies to incur inefficient costs to avoid the same fate;
- It incentivizes the FTC to impose remedies via consent order that a court might not sustain; and
- It may induce companies that would be found by a court not to have violated the statute to admit liability.

These largely hidden, underappreciated effects are, collectively, enormously distorting. And they feedback into the process, reinforcing the institutional dynamics that lead to such outcomes in the first place. In short, the FTC's discovery process greatly magnifies its already vast discretion to make substantive decisions about the evolution of Section 5 doctrine (or quasi-doctrine).

---

[93] Invention Submission, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing Fed. Trade Comm'n v. Carter, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

[94] *Re: LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand; and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand (*Apr. 20, 2012), 5, *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./102-3099-lab-md-letter-ruling-04202012.pdf.

At the same time, there is reason to believe that the rate of CID issuance, and the scope of CIDs issued, are (far) greater than optimal.

In order to issue a CID pursuant to an OR, staff need not present the authorizing Commissioner with a theory of the case or anything approaching "probable cause" for the CID; rather, the OR effectively takes care of that (although without anything like the specificity required of, say, a subpoena), and staff need only assert that the CID is in furtherance of an OR. The other Commissioners do not have an opportunity to vote on the issuance of the CID and would not likely even know about the investigation. Even if dissenting staff members attempt to notify Commissioners,[95] it may be difficult, at this early stage, for Commissioners to recognize the doctrinal or practical significance of the cases the staff is attempting to bring, and thus to provide any meaningful check upon the discretion of the staff to use the discovery process to coerce settlements.

Thus, because of omnibus resolutions, a great number of investigations — encompassing a great number of costly CIDs — are not presented to the other Commissioners to determine whether the investigation is an appropriate use of the agency's resources or whether the legal basis for the case is sound. In many cases, the other Commissioners may not even see the case until a settlement has been negotiated as a *fait accompli*.

The bar for issuing CIDs pursuant to an omnibus resolution is extremely low. Nominally the CID request must fall within the agency's authority and be relevant to the investigation that authorizes it. But the FTC has enormous discretion in determining whether a specific compulsory demand is relevant to an investigation, and it need not have "a justifiable belief that wrongdoing has actually occurred."[96]

For example, the Commission's telemarketing resolution authorized compulsory process

> [t]o determine whether unnamed telemarketers, sellers, or others assisting them have engaged in or are engaging in: (1) unfair or deceptive acts or practices in or affecting commerce in violation of Section 5 of the Federal Trade Commission Act; and/or (2) deceptive or abusive telemarketing acts or practices in violation of the Commission's Telemarketing Sales Rule, including but not limited to the provision of substantial assistance or support — such as mailing lists, scripts, merchant accounts, and other information, products, or services — to telemarketers engaged in unlawful practices. The investigation is also to determine

[95] Operating Manual § 3.5.1.1 ("Dissenting staff recommendations regarding compulsory process, compliance, consent agreements, proposed trade regulation rules or proposed industrywide investigations should be submitted to the Commission by the originating offices, upon the request of the staff member.").

[96] United States v. Morton Salt Co., 338 U.S. 632, 642 (1950).

> whether Commission action to obtain redress for injury to consumers or others would be in the public interest.[97]

Pursuant to this OR, the Commission issued a CID to Western Union. Western Union challenged the CID on the grounds that it was unrelated to the OR (among other things). The FTC, in denying the motion to quash, claimed that "[t]he resolution… includes investigations of telemarketers or sellers as well as entities such as Western Union who may be providing substantial assistance or support to telemarketers or sellers." While the OR does mention "assistance or support," it doesn't specify any companies by name and doesn't specify that payment processors provide the sort of support it contemplates. In fact, it is fairly clear from even the impressively broad characterization of these in the OR — "mailing lists, scripts, merchant accounts, and other information, products, or services" — that the ancillary processing of payment transactions by legitimate companies was not really contemplated.

Nevertheless, the standard of review for the relevance of CIDs — in the rare instance that they are challenged at all — is extremely generous to the agency. As the Commission notes in its *Western Union* decision:

> In the context of an administrative CID, "relevance" is defined broadly and with deference to an administrative agency's determination. An administrative agency is to be accorded "extreme breadth" in conducting an investigation. As the D.C. Circuit has stated, the standard for judging relevance in an administrative investigation is "more relaxed" than in an adjudicatory proceeding. As a result, the agency is entitled to the documents unless the CID recipient can show that the agency's determination is "obviously wrong" or the documents are "plainly irrelevant" to the investigation's purpose. We find that Western Union has not met this burden.[98]

Finally, administrative challenges to CIDs are public proceedings, which itself presents a substantial bar to their review. Companies subject to investigations by the FTC are, not surprisingly, reluctant to reveal the existence of such an investigation publicly. While the immense breadth and vagueness of the ORs authorizing compulsory process in an investigation, the ease with which CIDs are issued, and the lack of a "belief of wrongdoing" requirement certainly mean that no wrongdoing *should* be inferred from the existence of an investigation or a CID, unfortunately public perception may not track these nuances. In the

---

[97] *Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others*, File No. 0123145 (Apr. 11, 2011), quoted in *In the Matter of December 12, 2012 Civil Investigative Demand Issue to the Western Union Company*, File No. 012 3145 (Mar. 4, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/unnamed-telemarketers-others/130404westernunionpetition.pdf (Citations omitted).

[98] *In the Matter of December 12, 2012 Civil Investigative Demand Issue to the Western Union Company* at 8. (Citing cases).

case of some publicly traded companies, the mere issuance of a CID may require disclosure.[99] But for other publicly traded companies and for all private companies such disclosure is not required. This means that, for these companies, there is an added deterrent to challenging a CID because doing so will cause it to be disclosed publicly when it otherwise would not be.

The combination of an exceedingly deferential standard of review, the need to exhaust administrative process before the very agency that issued the OR and CID *before* gaining access to an independent Article III tribunal, the risk of reputational harms, and the massive compliance costs combine to ensure that very few CIDs are ever challenged. This only reinforces FTC staff's incentives to issue CIDs, and to do so with an increasingly tenuous relationship to the Commission-approved resolution authorizing them.

The absence of effective oversight on this process creates a further problem. FTC staff have the power to issue Voluntary Access Letters requesting the same documents as a CID without *any* Commissioner involvement — or even (at least on paper) the possibility that a dissenting staff member can notify a Commissioner of her objections.[100] While these requests are nominally voluntary, the omnipresent threat of compelled discovery means that recipients virtually always comply with these requests, although they do often initiate a discussion between staff and recipients that may result in a narrowing of the requests' scope. Voluntary Access Letters are subject to even less scrutiny than CIDs, and there is virtually no way for any of the FTC's oversight bodies (Congress, the courts, the public, the executive branch, etc.) to monitor their use.

Investigations and Reporting on Investigations

The Clarifying Legality & Enforcement Action Reasoning (CLEAR) Act

While identifying the problems with the Commission's investigation and CID process is fairly straightforward, identifying solutions is not so straightforward. A critical first step, however, would be imposing greater transparency requirements on the Commission's investigation practices.

---

[99] *See, e.g.*, Deborah S. Birnbach, *Do You Have to Disclose a Government Investigation?*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION (May 21, 2016), https://corpgov.law.harvard.edu/2016/04/09/do-you-have-to-disclose-a-government-investigation/.

[100] Again, Operating Manual Section 3.3.5.1.1 requires that "[d]issenting staff recommendations… be submitted to the Commission by the originating offices, upon the request of the staff member," but does not include voluntary assistance letters in the list of covered subjects, only "compulsory process."

Rep. Brett Guthrie's (R-KY) proposed CLEAR Act (H.R. 5109)[101] would require the FTC to report annually to Congress on the status of its investigations, including the legal analysis supporting the FTC's decision to close some investigations without action. This requirement would not require the Commission to identify its targets, thus preserving the anonymity of the firms in question.

VALUE OF THE BILL: Better Reporting of FTC Enforcement Trends

The FTC used to provide somewhat clearer data on the number of enforcement actions it took every year, classifying each by product and "type of matter."[102] The FTC's recent "Annual Highlights" reports do not include even this level of data on its enforcement actions. [103] But neither includes the basic data required by the CLEAR Act on the number of investigations commenced, closed, settled or litigated. Without hard data on this, it is difficult to assess how the FTC's enforcement approach works, the relationship between the agency's investigations and enforcement actions, and how these has changed over time. While the bill does not specifically mention consent decrees among the items that must be reported to Congress, it does require that the report include "the disposition of such investigations, if such investigations have concluded and resulted in official agency action," which would include consent decrees.

RECOMMENDATION: Add Discovery Tools to the Required Reporting

The bill omits, however, one of the most important aspects of the FTC's operations, which is very easily quantifiable: the FTC's use of its various discovery tools. The FTC should, in addition, have to produce aggregate statistics on its use of discovery tools, excluding the specific identity of the target, but including, for example:

- The source of the investigation (*e.g.*, Omnibus Resolution, consumer complaint, etc.);
- The volume of discovery requested;
- The volume of discovery produced;
- The time elapsed between the initiation of the investigation and the request(s);
- The time elapsed between the request(s) and production;
- Estimated cost of compliance (as volunteered by the target);

---

[101] The Clarifying Legality and Enforcement Action Reasoning Act, H.R. 5109, 114th Cong. (2016) [hereinafter CLEAR Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5109/text.

[102] *See. e.g.,* 1995 Annual Report at 49, https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-1995/ar1995_0.pdf.

[103] Fed. Trade Comm'n, FTC Annual Reports, https://www.ftc.gov/policy/reports/policy-reports/ftc-annual-reports.

- The specific tool(s) used to authorize the investigation and production request(s) (*e.g.*, Omnibus Resolution, CID, Voluntary Access Letter, etc.);
- Who approved the investigation and production request(s) (*e.g.*, a single Commissioner, the full Commission, the Bureau Director, the staff itself, etc.);
- The approximate size (number of employees) and annual revenues of the target business (to measure effects on small businesses); and
- The general nature of the issue(s) connected to the investigation and production request(s).

This reporting could be largely automated from the FTC database used to log investigations, discovery requests and resulting production of documents. And, of course, the FTC should have such a flexible and usable database if it does not already. Once created, it should be relatively easy to make the data public, as it will require little more than obscuring the identity of the target, putting the size of the company in ranges, and ensuring that the metadata identifying the relevant issues is sufficiently high level (e.g., "data security" rather than "PED skimming").

VALUE OF THE BILL: What is *Not* Prohibited Is a Crucial Form of Guidance

Clarity as to what the law does *not* prohibit may be a more important hallmark of the Evolutionary Model (the *true* common law), than is specificity as to what the law does prohibit.

The FTC used to issue closing letters regularly but stopped providing meaningful guidance at least since the start of this Administration. The FTC Operating Manual already requires staff to produce a memo justifying closure of any investigation that has gone beyond the initial stage, thus requiring the approval of the Bureau Directors to expand into a full investigation, that "summarize[s] the results of the investigation, discuss[es] the methodology used in the investigation, and explain[s] the rationale for the closing."[104]

In other words, the staff already, in theory, does the analysis that would be required by the bill (at least for cases that merit being continued beyond the 100 hours allowed for initial phase consumer protection investigations);[105] they simply do not share it. Thus, at most, the bill would require (i) greater rigor in the memoranda that staff already writes, (ii) that some version of memoranda be included in the annual report, edited to obscure the company's identity, and (iii) that *some* analysis be written for initial phase cases that may be closed without any internal memoranda. And this last requirement should not be difficult for the staff to satisfy, since cases that did not merit full investigations ought to raise simpler legal issues.

---

[104] Operating Manual § 3.2.4.1.1 (consumer protection) & § 3.2.4.1.2 (competition)

[105] Operating Manual § 3.2.2.1.

For example, in 2007, the FTC issued a no-action letter closing its investigation into Dollar Tree Stores that offers a fair amount of background on the issue: "PED skimming," the tampering with of payment card PIN entry devices (PEDs) used at checkout that allowed hackers to steal customers' card information and thus make fraudulent purchases.[106] The FTC explained its decision to close the Dollar Tree Stores investigation at length, listing the factors considered by the FTC:

> the extent to which the risk at issue was reasonable foreseeable at the time of the compromise; the nature and magnitude of the risk relative to other risks; the benefits relative to the costs of protecting against the risk; Dollar Tree's overall data security practices, the duration and scope of the compromise; the level of consumer injury; and Dollar Tree's prompt response to the incident.[107]

The letter went on to note:

> We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. The staff notes that, in recent months, the risk of PED skimming at retain locations has been increasingly identified by security experts and discussed in a variety of public and business contexts. We also understand that some businesses have now taken steps to improve physical security to deter PED skimming, such as locking or otherwise securing PERs in checkout lanes; installing security cameras or other monitoring devices; performing regular PED inspections to detect tampering, theft, or other misuse; and/or replacing older PEDs with newer tamper-resistant and tamper-evident models. We hope and expect that all businesses using PEDs in their stores will consider implementing these and/or other reasonable and appropriate safeguards to secure their systems.[108]

The FTC has issued only one closing letter in standard data security cases since its 2007 letter in *Dollar Tree Stores* — and, apparently, about the same issue. In 2011, the FTC issued a letter closing its investigation of the Michaels art supply store chain.[109] The letter offers essentially no information about the investigation or analysis of the issues involved — in marked contrast to the *Dollar Tree Stores* letter. But based on press reports from 2011, the issue appears to have been the same as in *Dollar Tree Stores*: "crooks [had] tampered with PIN

---

[106] Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (June 5, 2001) *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf.

[107] *Id.* at 2.

[108] *Id.*

[109] Letter from Maneesha Mithal, Associate Director of Fed. Trade Comm'n to Lisa J. Sotto, Counsel to Michael's Stores, Inc. (June 5, 2001) *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-stores-inc./120706michaelsstorescltr.pdf.

pads in the Michaels checkout lanes, allowing them to capture customers' debit card and PIN numbers."[110]

Once again, the FTC has become increasingly unwilling to constrain its own discretion, even in the issuance of closing letters that do not bar the FTC from taking future enforcement actions. This underscores not only the value of the CLEAR Act, but also of the challenge in getting the FTC to take seriously the bill's requirement that annual reports include, "for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation."[111]

RECOMMENDATION: Require the Bureau of Economics to Be Involved

Wherever possible, Congress should specify that the Bureau of Economics be involved in the making of important decisions, and in the production of important guidance materials. Absent that instruction, the FTC, especially the Bureau of Consumer Protection, will likely resist fully involving the Bureau of Economics in its processes. The simplest way to make this change is as follows:

> For each such investigation that was closed with no official agency action, a description sufficient to indicate the legal ***and economic*** analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

Of course, there will be many cases where the economists have essentially nothing to say. The point is not that each case merits detailed economic analysis. Rather, the recommendation is intended to ensure that, at the very least, the *opportunity* to produce and disseminate a basic economic analysis by the BE is built into the enforcement process.

Moreover, if an economic analysis is deemed appropriate, the determination of what constitutes an appropriate *level* of analysis should be made by the Bureau of Economics alone. For example, in the *Dollar Tree Stores* letter quoted above, it would have been helpful if the letter had provided *some* quantitative analysis as to the factors mentioned in the letter. To illustrate this point, one might ask the following questions about the factors identified in *Dollar Tree Stores*:

- "the extent to which the risk at issue was reasonably foreseeable at the time of the compromise" and "the nature and magnitude of the risk relative to other

---

[110] Elisabeth Leamy, *Debit Card Fraud Investigation Involving Michaels Craft Stores PIN Pads Spreads to 20 US States*, ABC NEWS (May 13, 2011) *available at* http://abcnews.go.com/Business/ConsumerNews/debit-card-fraud-michaels-crafts-customers-info-captured/story?id=13593607.

[111] CLEAR Act, *supra* note 101.

risks" — ***How widely known was the vulnerability generally at that time? How fast was awareness spreading among similarly situated companies? How likely was the vulnerability to occur?***

- "the benefits relative to the costs of protecting against the risk" — ***Given the impossibility of completely eradicating risk, how much ex ante "protection" would have been sufficient? Given the* ex ante *uncertainty of any particular risk occurring, how much would it have cost to mitigate against all such risks, not just the one that actually materialized?***
- "Dollar Tree's overall data security practices" — ***How much did the company spend? How else do its practices compare to its peers? How can good data security be quantified?***
- "the duration and scope of the compromise" — ***How long? How many users?***
- "the level of consumer injury" — ***Can this be quantified specifically to this case? Or can injury be extrapolated from reliably representative samples of similar injury?***
- "Dollar Tree's prompt response to the incident" — ***Just how prompt was it, in absolute terms? And relative to comparable industry practice?***

Given the general scope of the FTC's investigations, it likely already collects the kind of data that could allow it to answer some, if not all, of these questions (and others as well). It may even have performed some of the requisite analysis. Why should the Commission's economists not have a seat at the table in writing the closing analysis? This could be perhaps the greatest opportunity to begin bringing the analytical rigor of law and economics to consumer protection.

Of course, the Commission may be (quite understandably) reluctant to include this data in company-specific closing letters — for the same reasons that investigations are supposed to remain confidential. But therein lies one of the chief virtues of the CLEAR Act: Instead of writing company-specific letters, the FTC could aggregate the information, obscure the identity of the company at issue in each specific case, and thus speak more freely about the details of its situation. Although the tension between the goals of providing analytical clarity and maintaining confidentiality for the subjects of investigation is obvious, it is not an insurmountable conflict, and thus no reason not to require more analysis and disclosure, in principle.

Finally, it is worth noting that if BE is to be competent in its participation in these investigations and the associated reports, it will need a larger staff of economists. Thus, as we discuss below, Congress should devote additional resources to the Commission that are specifically earmarked for hiring additional BE staff.[112]

[112] *See infra* note 123.

RECOMMENDATION: Attempt to Make the FTC Take the Analysis Requirement Seriously

We recommend that Congress emphasize *why* such reporting is important with something like the following language, added either to Congressional findings or made clear in the legislative history around the bill:

- Guidance from the Commission as to what is *not* illegal may be the most important form of guidance the Commission can offer; and
- To be truly useful, such guidance should hew closely the FTC's applicable Policy Statements.

We further recommend that Congress carefully scrutinize the FTC's annual reports issued under the CLEAR Act in oral discussions at hearings and in written questions for the record. Indeed, *not* doing so will indicate to the FTC that Congress is not really serious about demanding greater analytical rigor.

RECOMMENDATION: Ensure that the Commission Organizes These Reports in a Useful Manner

The legal analysis section of the bill is markedly different from the other three sections. The first two sections require simple counts of investigations commenced and closed with no action. The third section ("disposition of such investigations, if such investigations have concluded and resulted in official agency action") can be satisfied with a brief sentence for each (or less). But the fourth section requires long-form analysis, which could run many pages for each case.

At a minimum, the FTC should do more than it does today to make it easy to identify which closing letters are relevant. Today, the Commission's web interface for closing letters is essentially useless. Letters are listed in reverse chronological order with no information provided other than the name, title and corporate affiliation of the person to whom the letter is addressed. There is no metadata to indicate what the letter is about (e.g., privacy, data security, advertising, product design) or what doctrinal issues (*e.g.,* unfairness, deception, material omissions, substantiation) the letter confronts. Key word searches for, say, "privacy" or "data security" produce zero results.

The CLEAR Act offers Congress a chance to demand better of the Commission. Congress should communicate what a *useful* discussion of closing decisions might look like — whether by including specific instructions in legislation, by addressing the issue in legislative history, or simply (and probably least effectively in the long term) by raising the issue regularly with the FTC at hearings. For instance, the text in the FTC's reports to Congress could be made publicly available in an online database tagged with metadata to make it easier for users to search for and find relevant closing letters.

Ideally, this database would be accessed through the same interface envisioned above for transparency into the FTC's discovery process, and would include the same metadata and

search tools. Thus, a user might be able to search for FTC enforcement actions and discovery inquiries regarding, say, data security practices in small businesses, in order to get a better sense of how the FTC operates in that area.

RECOMMENDATION: Require the FTC to Synthesize Closing Decisions and Enforcement Decisions into Doctrinal Guidelines

When the FTC submitted the Unfairness Policy Statement to Congress, it noted, in its cover letter:

> In response to your inquiry we have therefore undertaken a review of the decided cases and rules and have synthesized from them the most important principles of general applicability. Rather than merely reciting the law, we have attempted to provide the Committee with a concrete indication of the manner in which the Commission has enforced, and will continue to enforce, its unfairness mandate. In so doing we intend to address the concerns that have been raised about the meaning of consumer unfairness, and thereby attempt to provide a greater sense of certainty about what the Commission would regard as an unfair act or practice under Section 5.[113]

This synthesis is what the FTC needs to do now — and could get close to doing, in part, through better organized reporting on its closing decisions — only on a more specific level of the component elements of each of its Policy Statements. This is essentially what the various Antitrust Guidelines issued jointly by the DOJ and the FTC's Bureau of Competition do. These are masterpieces of thematic organization. Consider, for example, from the 2000 Antitrust Guidelines for Collaborations Among Competitors, this sample of the table of contents:

> **3.34** Factors Relevant to the Ability and Incentive of the Participants and the Collaboration to Compete
> - **3.34(a)** Exclusivity
> - **3.34(b)** Control over Assets
> - **3.34(c)** Financial Interests in the Collaboration or in Other Participants
> - **3.34(d)** Control of the Collaboration's Competitively Significant Decision Making
> - **3.34(e)** Likelihood of Anticompetitive Information Sharing
> - **3.34(f)** Duration of the Collaboration

> **3.35** Entry

> **3.36** Identifying Procompetitive Benefits of the Collaboration
> - **3.36(a)** Cognizable Efficiencies Must Be Verifiable and Potentially Procompetitive

[113] UPS, *supra* note 9.

3.36(b) Reasonable Necessity and Less Restrictive Alternatives
3.37 Overall Competitive Effect[114]

The guidelines are rich with examples that illustrate the way the agencies will apply their doctrine. As noted in the introduction, these guidelines are one level down the Doctrinal Pyramid: They explain how the kind of concepts articulated at the high conceptual level of, say, the FTC's UDAP policy statements, can actually be applied to real world circumstances.[115]

One obvious challenge is that the antitrust guidelines synthesize litigated cases, of which the FTC has precious few on UDAP matters. This makes it difficult, if not impossible, for the FTC to do *precisely* the same thing on UDAP matters as the antitrust guidelines do. But that does not mean the FTC could not benefit from writing "lessons learned" retrospectives on its past enforcement efforts and closing letters.

Importantly, publication of these guidelines would not actually be a constraint upon the FTC's discretion; it would merely require the Commission to better explain the rationale for what it has done in the past, connecting that arc across time. Like policy statements and consent decrees, guidelines are not technically binding upon the agency. Yet, in practice, they would steer the Commission in a far more rigorous way than its vague "common law of consent decrees [or of congressional testimony or blog posts]." It would allow the FTC to build doctrine in an analytically rigorous way as a second-best alternative to judicial decision-making — and, of course, as a supplement to judicial decisions, to the extent they happen.

RECOMMENDATION: Ensure that Defendants Can Quash Subpoenas Confidentially

Among the biggest deterrents to litigation today is companies' reluctance to make public investigations aimed at them. But a company wishing to challenge the FTC's overly broad investigative demands effectively must accede to public disclosure because the FTC has the discretion to make such fights public.

Specifically, FTC enforcement rules currently allow parties seeking to quash a subpoena to ask for confidential treatment for their motions to quash, but the rules also appear to set public disclosure as the default:

---

[114] FED. TRADE COMM'N & DEP'T OF JUSTICE, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS ii (Apr. 2000), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

[115] *See supra* note 12.

> (d) **Public disclosure**. All petitions to limit or quash Commission compulsory process and all Commission orders in response to those petitions shall become part of the public records of the Commission, except for information granted confidential treatment under § 4.9(c) of this chapter.[116]

The referenced general rule on confidentiality gives the FTC's General Counsel broad discretion in matters of confidentiality:

> (c) **Confidentiality and in camera material**.
>
> (1) Persons submitting material to the Commission described in this section may designate that material or portions of it confidential and request that it be withheld from the public record. All requests for confidential treatment shall be supported by a showing of justification in light of applicable statutes, rules, orders of the Commission or its administrative law judges, orders of the courts, or other relevant authority. **The General Counsel or the General Counsel's designee will act upon such request with due regard for legal constraints and the public interest**.[117]

Setting the default to public disclosure for such disputes is flatly inconsistent with the FTC's general policy of keeping investigations nonpublic:

> While investigations are generally nonpublic, Commission staff may disclose the existence of an investigation to potential witnesses or other third parties to the extent necessary to advance the investigation.[118]

This is the right balance: Commission staff should *sometimes* be able to disclose aspects of an investigation. It should *not* be able to coerce a company into settling, or complying with additional discovery, in order to avoid bad press. Even if a company calculates that bad press is inevitable, if the FTC seems determined to extract a settlement, disclosing the investigation earlier can increase the direct expenses and reputational costs incurred by the company by stretching out the total length of the fight with the Commission for months or years longer.

---

[116] 16 C.F.R. § 2.10(d).

[117] 16 C.F.R. § 4.9(c)(1).

[118] 16 C.F.R. § 2.6; *See also* Federal Trade Commission, *Operating Manual*, Section 3.3.1 (To promote orderly investigative procedures and to protect individuals or business entities under investigation from premature adverse publicity, the Commission treats the fact that a particular proposed respondent is under investigation and the documents and information submitted to or developed by staff in connection with the investigation as confidential information that can be released only in the manner and to the extent authorized by law and by the Commission. In general, even if a proposed respondent in a nonpublic investigation makes a public disclosure that an investigation is being conducted, Commission personnel may not acknowledge the existence of the investigation, or discuss its purpose and scope or the nature of the suspected violation.)

We propose that the default be switched, so that motions to quash are generally kept under seal except in exceptional circumstances.

Economic Analysis of Investigations, Complaints, and Consent Decrees

No Bill Proposed

> The Federal Trade Commission's Bureau of Economics' (BE) role as an independent and expert analyst is one of the most critical features of the FTC's organizational structure in terms of enhancing its performance, expanding its substantive capabilities, and increasing the critical reputational capital the agency has available to promote its missions.[119]
>
> *Former FTC Commissioner Joshua Wright, 2015*

Commissioner Wright wrote as a veteran of both the Bureau of Economics and the Bureau of Competition. He was only the fourth economist to serve as FTC Commissioner (following Jim Miller, George Douglas and Dennis Yao) and the first JD/PhD. His 2015 speech, "On the FTC's Bureau of Economics, Independence, and Agency Performance," marked the beginning of an effort to bolster the role of the Bureau of Economics in the FTC's decision-making, especially in consumer protection matters. Wright warned, pointedly, that the FTC has "too many lawyers, too few economists," calling this "a potential threat to independence and agency performance."[120]

Unfortunately, this was only a beginning: shortly after delivering this speech, Wright resigned from the Commission to return to teaching law and economics. For now, at least, the task of bolstering economic analysis at the Commission falls to Congress.

The RECS Act's proposal that BE be involved in any recommendation for new legislation or regulatory action is an important step towards this goal, but it is too narrow.[121] It does not address the need to bolster the FTC's role in the institutional structure of the agency, or its role in enforcement decisions. The following chart (from Wright's speech) ably captures the first of these problems:

Number of Attorneys to Economists at the FTC from 2003 to 2013[122]

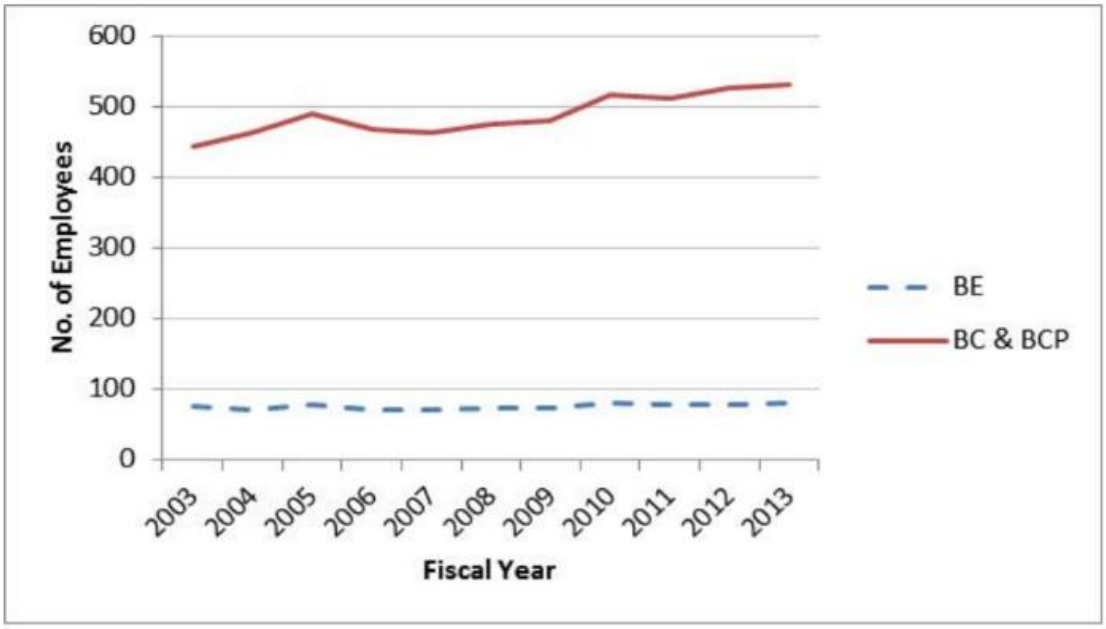
---

[119] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, at 1 (Aug. 6, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/695241/150806bestmtwright.pdf.

[120] *Id.* at 5.

[121] *See infra* at 54.

[122] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, *supra* note 119, at 6.



RECOMMENDATION: Hire More Economists

Wright recommends:

> Hiring more full-time economists is one obvious fix to the ratio problem. There are many benefits to expanding the economic capabilities of the agency. Many cases simply cannot be adequately staffed with one or two staff economists. **Doubling the current size of BE** would be a good start towards aligning the incentives of the Commission and BE staff with respect to case recommendations. While too quickly increasing the size of BE staff might dilute quality, a gradual increase in staffing coupled with a pay increase and a commitment to research time should help to keep quality levels at least constant.[123]

We wholeheartedly endorse former Commissioner Wright's recommendation.

RECOMMENDATION: Require BE to Comment Separately on Complaints and Consent Orders

In the case of complaints and consent orders issued by the Commission, we recommend that Congress require the Commission to amend its Rules of Practice to require that the Bureau of Economics provide a *separate* economic assessment of the complaint or consent order in conjunction with each. This proposal is consistent with former Commissioner Wright's similar recommendation:

---

[123] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, *supra* note 119, at 11.

> I suggest the FTC consider interpreting or amending FTC Rule of Practice 2.34 to mandate that BE publish, in matters involving consent decrees, and as part of the already required "explanation of the provisions of the order and the relief to be obtained," a separate explanation of the economic analysis of the Commission's action. The documents associated with this rule are critical for communicating the role that economic analysis plays in Commission decision-making in cases. In many cases, public facing documents surrounding consents in competition cases simply do not describe well or at all the economic analysis conducted by staff or upon which BE recommended the consent.[124]

In order to perform its desired function, this "separate explanation" would be authored and issued by the Bureau of Economics, and not subject to approval by the Commission. The document would express BE's independent assessment (approval or rejection) of the Commission's proposed complaint or consent order, provide a high-level description of the specific economic analyses and evidence relied upon in its own recommendation or rejection of the proposed consent order, and offer a more general economic rationale for its recommendation.

Requiring BE to make public its economic rationale for supporting or rejecting a complaint or consent decree voted out by the Commission would offer a number of benefits. In general, such an analysis would both inform the public and demand rigor of the Commission. As former Commissioner Wright noted,

> First, it offers BE a public avenue to communicate its findings to the public. Second, it reinforces the independent nature of the recommendation that BE offers. Third, it breaks the agency monopoly the FTC lawyers currently enjoy in terms of framing a particular matter to the public. The internal leverage BE gains by the ability to publish such a document… will also provide BE a greater role in the consent process and a mechanism to discipline consents that are not supported by sound economics…, minimizing the "compromise" recommendation that is most problematic in matters involving consent decrees.[125]

Wright explains this "compromise recommendation" problem in detail that bears extensive quotation and emphasis here:

> Both BC attorneys and BE staff are responsible for producing a recommendation memo. The asymmetry is at least partially a natural result of the different nature of the work that lawyers and economists do. But it is important to note that one consequence of this asymmetry, whatever its cause, is that it creates the potential to weaken BE's independence. BE maintains a high level of integrity and independence over core economic tasks – e.g., economic modeling and framing, statistical analyses, and assessments of outside economic work – yet when it comes

[124] *Id.* at 11-12.

[125] *Id.* at 11.

> to the actual policy recommendation, **I think it is fair to raise the question whether the Commission always receives unfiltered recommendations when BE dissents from the recommendation of BC or BCP staff.**
>
> One example of this phenomenon is the so-called "compromise recommendation," that is, a BE staff economist might recommend the FTC accept a consent decree rather than litigate or challenge a proposed merger when the underlying economic analysis reveals very little actual economic support for liability. In my experience, **it is not uncommon for a BE staff analysis to convincingly demonstrate that competitive harm is possible but unlikely, but for BE staff to recommend against litigation on those grounds, but in favor of a consent order**. The problem with this compromise approach is, of course, that a recommendation to enter into a consent order must also require economic evidence sufficient to give the Commission reason to believe that competitive harm is likely. This type of "compromise" recommendation in some ways reflects the reality of BE staff incentives. Engaging in a prolonged struggle over the issue of liability with BC and BC management is exceedingly difficult when the economist is simply outmanned. It also ties up already scarce BE resources on a matter that the parties are apparently "willing" to settle.[126]

The ability of BC or BCP staff to dilute the analysis of BE staffers in a combined compromise recommendation renders moot this provision of the operating manual:

> Dissenting staff recommendations regarding compulsory process, compliance, consent agreements, proposed trade regulation rules or proposed industrywide investigations should be submitted to the Commission by the originating offices, upon the request of the staff member.[127]

For this provision to have any effect, there must be a separate dissenting staff recommendation that can be seen by Commissioners — and, ideally, also made public.

RECOMMENDATION: Require BE to Comment on Upgrading Investigations

Similarly, we recommend enhancing BE's role earlier in the investigation process: at the point where the Bureau Director decides whether to upgrade an initial (Phase I) investigation to a full investigation. This is a critical inflection point in the FTC's investigative process for three reasons:

1. In principle, the staff is not supposed to negotiate consent decrees during the initial investigation phase;
2. In principle, the staff is not supposed to use compulsory discovery process during the initial investigation phase, meaning a target company's cooperation until this point is at least theoretically voluntary; and

---

[126] *Id.* at 7-8.

[127] Operating Manual § 3.3.5.1.1.

3. Either the decision to open a formal investigation or the subsequent issuance of CIDs may trigger a public company's duty to disclose the investigation in its quarterly securities filings.

It is also likely the point at which the staff determines (or at least begins to seriously consider) whether or not the Commission is likely to approve a staff recommendation to issue a complaint against any of the specific targets of the investigation.

For all these reasons, converting an initial investigation to a full investigation gives the staff enormous power to coerce a settlement. This decision deserves far more rigorous analysis than it currently seems to receive.

When the BC or BCP staff proposes to their Bureau director that an initial investigation be expanded into a full investigation, the FTC Operating Manual requires a (confidential) memorandum justifying a decision, but does *not* formally require the Bureau of Economics, or require that the analysis performed by any FTC staff correspond to two of the three requirements of Section 5(n) or the materiality requirement of the Deception Policy Statement:

> 3.5.1.4 Transmittal Memorandum
>
> The memorandum requesting approval for full investigation should clearly and succinctly explain the need for approval of the full investigation, including a discussion of relevant factors among the following:
>
> (1) A description of the practices and their impact on consumers and/or on the marketplace;
> (2) Marketing area and volume of business of the proposed respondent and the overall size of the market;
> (3) Extent of consumer injury inflicted by the practices to be investigated, the benefits to be achieved by the Commission action and/or the extent of competitive injury;
> (4) When applicable, an explanation of how the proposed investigation meets objectives and, where adopted, case selection criteria or the program to which it has been assigned;
> (5) When applicable, responses to the policy protocol questions (see OM Ch. 2);[128]

We recommend modifying this in two ways. First, while approving a complaint or a consent decree should absolutely require a separate recommendation from the Bureau of Economics, requiring such a recommendation merely to convert an initial investigation to a full investigation might well pose too great a burden on BE's already over-taxed resources. But that is no reason why the FTC rules should not at least give BE the *opportunity* to write a

[128] Operating Manual § 3.3.5.1.4 (emphasis added).

separate memorandum if it so desires. Having this written recommendation shared with Commissioners would serve as an early warning system, alerting them to potentially problematic cases being investigated by BCP or BC staff *before* the staff has extracted a consent decree — something that regularly has effectively happened by the time the Commission votes on whether to authorize a complaint. Thus, giving BE the opportunity to be involved at this early stage may be critical to scrutinizing the FTC's use of consent decrees.

Second, there is no reason that the memorandum prepared by either BC or BCP staff should not correspond to the doctrinal requirements of the relevant authority. The Operating Manual falls well short of this by merely requiring some analysis of the "[e]xtent of consumer injury." Why not countervailing benefit and reasonable avoidability, too, for Unfairness cases? And materiality in Deception cases? And the various other factors subsumed in the consumer welfare standard of the rule of reason, for Unfair Methods of Competition Cases?

That this would be only an *initial* analysis that will remain confidential under the Commission's rules is all the more reason it should not be a problem for the Staff to produce.

Economic Analysis in Reports & "Recommendations"

The Revealing Economic Conclusions for Suggestions (RECS) Act

Rep. Mike Pompeo's (R-KS) bill (H.R. 5136)[129] would require the FTC to include, in "any recommendations for legislative or regulatory action," analysis from the Bureau of Economics including:

> [T]he rationale for the Commission's determination that private markets or public institutions could not adequately address the issue, and that its recommended legislative or regulatory action is based on a reasoned determination that the benefits of the recommended action outweigh its costs.

Valuable as this is, the bill should be expanded to encompass other Commission pronouncements that aren't, strictly, "recommendations for legislative or regulatory action."

VALUE OF THE BILL: Bringing Rigor to FTC Reports, Testimony, etc.

The lack of economic analysis in support of "recommendations for legislative or regulatory action" has grown more acute with time — not only in the FTC's reports but also in its testimony to Congress.

Section 6(b) of the FTC Act gives the Commission the authority "to conduct wide-ranging economic studies that do not have a specific law enforcement purpose" and to require the

[129] The Revealing Economic Conclusions for Suggestions Act, H.R. 5136, 114th Cong. (2016) [hereinafter RECS Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5136/text.

filing of "annual or special … reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of any company over which the FTC has jurisdiction, except insurance companies. This section is a useful tool for better understanding business practices, particularly those undergoing rapid technological change. But it is only as valuable as the quality of the analyses these 6(b) reports contain. And typically they are fairly short on economic analysis, especially concerning consumer protection matters.

The FTC has consistently failed to include any apparent, meaningful role for the Bureau of Economics in its consumer protection workshops or in the drafting of the subsequent reports. Nor has the FTC explored the adequacy of existing legal tools to address concerns raised by its reports. For example, the FTC's 2014 workshop, "Big Data: A Tool for Inclusion or Exclusion?," included not a single PhD economist or BE staffer.[130] The resulting 2016 report includes essentially just two footnotes on economics.[131] Commissioner Ohlhausen dissented, noting that

> Concerns about the effects of inaccurate data are certainly legitimate, but policymakers must evaluate such concerns in the larger context of the market and economic forces companies face. Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap….
>
> To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals. Today's report enriches the conversation about big data. My hope is that future participants in this conversation will test hypothetical harms with economic reasoning and empirical evidence.[132]

---

[130] Fed. Trade Comm'n, Public Workshop: Big Data: A Tool for Inclusion or Exclusion? (Sep. 15, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[131] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES FTC REPORT (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[132] *Id.* at A-1 to A-2.

The Commission's 2016 PrivacyCon conference did include several economists on a panel devoted to the "Economics of Privacy & Security."[133] But, as one of the event's discussants, Geoffrey Manne, noted:

> One of the things I would say is that it's a little bit unfortunate we don't have more economists and engineers talking to each other. As you might have gathered from the last panel, an economist will tell you that merely identifying a problem isn't a sufficient basis for regulating to solve it, nor does the existence of a possible solution mean that that solution should be mandated. And you really need to identify real harms rather than just inferring them, as James Cooper pointed out earlier. And we need to give some thought to self-help and reputation and competition as solutions before we start to intervene….
>
> So we've talked all day about privacy risks, biases in data, bad outcomes, problems, but we haven't talked enough about beneficial uses that these things may enable. So deriving policy prescriptions from these sort of lopsided discussions is really perilous.
>
> Now, there's an additional problem that we have in this forum as well, which is that the FTC has a tendency to find justification for enforcement decisions in things that are mentioned at workshops just like these. So that makes it doubly risky to be talking [] about these things without pointing out that there are important benefits here, and that the costs may not be as dramatic as it seems [just] because we're presenting these papers describing them.[134]

As Manne notes, as a practical matter, these workshops and reports are often used by the Commission either to make legislative recommendations or to define FTC enforcement policy by recommending industry best practices (which the agency will effectively enforce). But, again, because they lack much in the way of economically rigorous analysis, these recommendations may not be as well-founded as they may be presumed to be.

In its 2000 Report to Congress, for example, the FTC called for comprehensive baseline legislation on privacy and data security.[135] Congress has not passed such legislation, but the FTC repeated the recommendation in its 2012 Privacy Report.[136] While that Report called

---

[133] Fed. Trade Comm'n, *Conference: PrivacyCon* (Jan. 14, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon.

[134] Fed. Trade Comm'n, *Transcript of the Remarks of Geoffrey A. Manne*, 19 (Jan. 14, 2016), *available at* https://www.ftc.gov/system/files/documents/videos/privacycon-part-5/ftc_privacycon_-_transcript_segment_5.pdf#page=18.

[135] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

[136] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012), *available at*

(cont.)

for significantly stricter legislation, less tied to consumer harm, it did *not* include any economic analysis by the FTC's Bureau of Economics. Indeed, by rejecting the harms-based model of the 2000 Report,[137] the 2012 report essentially dismisses the *relevance* of economic analysis, either in the report itself or in case-by-case adjudication.

In his dissent, Commissioner Rosch warned about the Report's reliance on unfairness rather than deception, noting that "'Unfairness' is an elastic and elusive concept. What is "unfair" is in the eye of the beholder…."[138] In effect, Rosch, despite his long-standing hostility to economic analysis,[139] was really saying that the Commission had failed to justify its *analysis* of unfairness. Rosch objected to the Commission's invocation of unfairness against harms that have not been clearly analyzed:

> That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982 [sic], Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm. In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted.[140]

Rosch contrasted the Report's reliance on unfairness with the Commission's Unfair Methods of Competition doctrine, which he called "self-limiting" because it was tied to analysis of market power.[141] Rosch lamented that,

> There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world. That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n). I would instead stand by what we have said

---

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[137] PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, *supra* note 135.

[138] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE*, supra* note 136, at C-3.

[139] *See e.g.*, J. Thomas Rosch, *Litigating Merger Challenges: Lessons Learned* (June 2, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/litigating-merger-challenges-lessons-learned/080602litigatingmerger.pdf ("any kind of economic analyses that require the use of mathematical formulae are of little persuasive value in the courtroom setting;" "when I see an economic formula my eyes start to glaze over."); *See generally* Joshua Wright, *Commissioner Rosch v. Economics, Again*, TRUTH ON THE MARKET (Oct. 7, 2008), *available at* https://truthonthemarket.com/2008/10/07/commissioner-rosch-v-economics-again/.

[140] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at C-4.

[141] *Id.* at C-5.

> and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.[142]

The proposed bill would help to correct these defects, and to ensure that FTC Reports, at least those containing legislative or rulemaking recommendations, are based on the rigorous analysis that should be expected of an expert investigative agency's policymaking — especially one that has arguably the greatest pool of economic talent found anywhere in government in America.

RECOMMENDATION: Require Analysis of Recommended Industry Best Practices

In this regard the proposed bill would be enormously beneficial, but it could, and should, do significantly more.

First and foremost, the term "recommendations for legislative or regulatory action" would not encompass the most significant FTC recommendations: those included in "industry best practices" publications and reports produced by the Commission. These documents purport to offer expert suggestions for businesses to follow in order to help them to protect consumer welfare and to better comply with the relevant laws and regulations. But the FTC increasingly treats these recommendations as soft law, not merely helpful guidance, in at least two senses:

1. The FTC uses these recommendations as the basis for writing its 20-year consent-decree requirements, including ones unrelated, or only loosely related, to the conduct at issue in an enforcement action; and
2. The FTC uses these recommendations as the substantive basis for enforcement actions — for example, by pointing to a company's failure to do something the FTC recommended as evidence of the unreasonableness of its practices.

Former Chairman Tim Muris notes this about the "voluntary" guidelines issued by the FTC in 2009 in conjunction with three other federal agencies, comparing them to the FTC's efforts to ban advertising to children:

> The FTC has been down this road before. Prodded by consumer activists in the late 1970s, the Commission sought to stop advertising to children…
>
> One difference between the current proposal and the old rulemaking — called Kid Vid — is that this time the agencies are suggesting that the standards be adopted "voluntarily" by industry. Yet can standards suggested by a government

[142] *Id.*

> claiming the power to regulate truly be "voluntary"? Moreover, at the same workshop that the standards were announced, a representative of one of the same activist organizations that inspired the 1970s efforts speculated that a failure to comply with the new proposal would provoke calls for rules or legislation.[143]

Regulation by leering glare is still regulation.

Informed by the trauma of its near-fatal confrontation with Congress at the end of the Carter administration, the FTC was long skittish about making recommendations for businesses in its reports, beyond high level calls for attention to issues like data security. That changed in 2009, however. The FTC has since issued a flurry of reports recommending best practices like "privacy by design" and "security by design," first generally, and then across a variety of areas, from Big Data to facial recognition.[144]

The FTC's recommendations to industry in its 2005 report on file-sharing were admirably circumspect:

> Industry should decrease risks to consumers through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.[145]

This is not to say that the FTC could not or should not have done more to address the very real problem of inadvertent online file-sharing. Indeed, one of the authors of this report has lauded the (Democratic-led) FTC for bringing its 2011 enforcement action against Frostwire[146] for designing its peer-to-peer file-sharing software in a way that deceived users into unwittingly sharing files.[147] Rather, it is simply to say that the FTC, in 2005, understood that a report was not a substitute for a rulemaking — *i.e.*, not an appropriate place to make "recommendations" for the private sector that would have any force of law.

By 2012 the FTC had lost any such scruples. Its Privacy Report, issued that year, is entitled "Recommendations for Businesses and Policymakers." The title says it all: The FTC di-

---

[143] *Statement of Timothy J. Muris, supra* note 14, at 11-13.

[144] BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION, *supra* note 131; FED TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[145] FED. TRADE COMM'N, PEER-TO-PEER FILE-SHARING TECHNOLOGY: CONSUMER PROTECTION AND COMPETITION ISSUES (2005), *available at* https://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf.

[146] Fed. Trade Comm'n v. Frostwire LLC, FTC File No. 112 3041, https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon (2011).

[147] *Prepared Statement of Berin Szóka, President of TechFreedom: Hearing Before the H. Energy & Commerce Comm.* 112th Cong. (2012), 23, *available at* https://techliberation.com/wp-content/uploads/2012/11/Testimony_CMT_03.29.12_Szoka.pdf.

rected its sweeping recommendations for "privacy by design" to both the companies it regulates and the elected representatives the FTC supposedly serves:

> The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation.[148]

Of course, the FTC added:

> To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.[149]

Also noteworthy is the contrast between the two reports in their analytical rigor. The file sharing report noted:

> The workshop panelists and public comments did not provide a sufficient basis to conclude whether the degree of risk associated with P2P file-sharing programs is greater than, equal to, or less than the degree of risk when using other Internet technologies.[150]

The 2012 report shows no such modesty, as Commissioner Rosch lamented in his dissent ("There does not appear to be any such limiting principle applicable to many of the recommendations of the Report.").[151]

In 2015, Commissioner Wright expressed dismay at this same problem in his dissent from the staff report on the Internet of Things Workshop:

> I dissent from the Commission's decision to authorize the publication of staff's report on its Internet of Things workshop ("Workshop Report") because the Workshop Report includes a lengthy discussion of industry best practices and recommendations for broad-based privacy legislation without analytical support to establish the likelihood that those practices and recommendations, if adopted, would improve consumer welfare….
>
> First…, merely holding a workshop — without more — should rarely be the sole or even the primary basis for setting forth specific best practices or legislative recommendations….

---

[148] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at iii.

[149] *Id*. at vii.

[150] PEER-TO-PEER FILE-SHARING TECHNOLOGY, *supra* note 145, at 12.

[151] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at C-5.

> Second, the Commission and our staff must actually engage in a rigorous cost-benefit analysis prior to disseminating best practices or legislative recommendations, given the real world consequences for the consumers we are obligated to protect….
>
> **The most significant drawback of the concepts of "security by design" and other privacy-related catchphrases is that they do not appear to contain any meaningful analytical content**…. An economic and evidence-based approach sensitive to [] tradeoffs is much more likely to result in consumer-welfare enhancing consumer protection regulation. To the extent concepts such as security by design or data minimization are endorsed at any cost — or without regard to whether the marginal cost of a particular decision exceeds its marginal benefits — then application of these principles will result in greater compliance costs without countervailing benefit. Such costs will be passed on to consumers in the form of higher prices or less useful products, as well as potentially deter competition and innovation among firms participating in the Internet of Things.[152]

The point illustrated by comparing these examples is the difficulty inherent in trying to require greater rigor from the FTC in recommendations to businesses when those recommendations can be either high level and commonsensical (as in 2005) or sweeping and effectively regulatory (as in 2012 and 2015). Thus, we recommend the following simple amendment to the proposed bill:

> [The FTC] shall not submit any ***proposed industry best practices, industry guidance or*** recommendations for legislative or regulatory action without [analysis]….

This wording would not apply to the kind of "recommendation" that the FTC made occasionally before 2009, as exemplified by the 2005 report. In any event, the bill's requirement is easily satisfied: essentially the FTC need only give the Bureau of Economics a role in drafting the report. Because this recommendation would not hamstring the FTC's enforcement actions, nor tie the FTC up in court, it should not be controversial, even if applied to proposed industry best practices and guidance.

Our proposed amendment would be simpler than attempting to broaden the definition of "regulatory action" beyond just rulemakings (which is how the FTC would likely limit its interpretation of the bill as drafted now) to include the kind of "regulatory action" that matters most: its use of reports to indicate how it will regulate through case by case enforcement, *i.e.*, its "common law of consent decrees."

---

[152] Dissenting Statement of Commissioner Joshua D. Wright, *Issuance of The Internet of Things: Privacy and Security in a Connected World Staff Report* (Jan. 27, 2015) (emphasis added), available at https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

RECOMMENDATION: Clarify the Bill's Language to Ensure It Applies to All FTC Reports

Another important difference between the 2000 and 2012 privacy reports is that the 2000 report is labelled "A Report to Congress," while the 2012 report is not and, indeed, barely mentions Congress. This reflects a little-noticed aspect of the way Section 6(f) is currently written, with subsection numbers added for clarity:

> (f) Publication of information; reports
>
> To [i] make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to [ii] make annual and special reports to the Congress and to submit therewith recommendations for additional legislation; and to [iii] provide for the publication of its reports and decisions in such form and manner as may be best adapted for public information and use.[153]

In other words, the Commission has shifted from relying upon 6(f)(ii) to 6(f)(i) and (iii). This distinction may seem unimportant, but it may cause the bill as drafted to be rendered meaningless, because the way it is worded could be read to apply only to 6(f)(ii). The bill would amend the existing proviso in Section 6(f) as follows:

> Provided [t]hat the Commission shall not submit any recommendations for legislative or regulatory action without an economic analysis by the Bureau of Economics….

The use of the words "submit" and "recommendations" clearly tie this proviso to 6(f)(ii). Thus, the FTC could claim that it need not include the analysis required by the bill unless it is specifically submitting recommendations to Congress, which it simply does not do anymore.

Instead we propose the following slight tweak to the bill's wording, to ensure that it would apply to the entirety of Section 6(f):

> Provided [t]hat the Commission shall not ***make*** any recommendations for legislative or regulatory action without an economic analysis by the Bureau of Economics…

This would require the participation of the Bureau of Economics in *all* FTC reports (that make qualifying recommendations), whatever their form. It would also require BE's participation in at least two other contexts where such recommendations are likely to be made: (i) Congressional testimony and (ii) the competition advocacy filings the Commission makes with state and local regulatory and legislative bodies, and with other federal regulatory

[153] 15 U.S.C. § 46(f)

agencies. This is a feature, not a bug: participation by BE is not something to be minimized; it should be woven into the fabric of *all* of the FTC's activities. As we have noted previously:

> The most important, most welfare-enhancing reform the FTC could undertake is to better incorporate sound economic- and evidence-based analysis in both its substantive decisions as well as in its process. While the FTC has a strong tradition of economics in its antitrust decision-making, its record in using economics in other areas is mixed.[154]

Because the bill does not in any way create a cause of action against the FTC for failing to comply with the requirement, it will not hamstring the FTC if the agency fails to take the bill's requirements seriously. That, if anything, is a weakness of the bill, but it is largely inevitable. It will always be up to the discretion of the Commission itself (subject, of course, to congressional oversight) to decide how much "economic analysis" is "sufficient" under the bill.

RECOMMENDATION: Require a Supermajority of Commissioners to Decide What Analysis is "Sufficient"

As written, the bill might do little more than shame the Chairman into involving the Bureau of Economics somewhat more in the writing of reports and the workshops that lead to them — if only because the bill might embolden a single Commissioner to object to the FTC's lack of analysis, as Commissioner Wright objected to the FTC's Internet of Things report.[155] This change in incentives for the Chairman and other commissioners, alone, may not significantly improve the analytical quality of the FTC's reports, given the hostility of the Bureau of Consumer Protection to economic analysis, although having *any* involvement by BE would certainly be an improvement.

Again, the question of "sufficiency" is inherently something that will be left to the Commission's discretion, but there is no principled reason that it has to be resolved through simple majority votes. On the other hand, giving a single Commissioner the right to veto an FTC "recommendation" as lacking a "sufficient" analytical basis might go too far.

We recommend striking a balance by requiring a supermajority (majority plus one, except in the case of a three-member Commission) of Commissioners to approve of the sufficiency of the analysis — essentially that this vote be taken, or at least recorded, separately from the vote on the issuance of the report itself. (The "sufficiency" vote would not stop the FTC from issuing a report.) At the same time, we recommend that the outcome of the "sufficien-

---

[154] Geoffrey A. Manne, *Humility, Institutional Constraints and Economic Rigor: Limiting the FTC's Discretion*, ICLE White Paper 2014-1 (Feb. 28, 2014) at 4, *available at* http://docs.house.gov/meetings/IF/IF17/20140228/101812/HHRG-113-IF17-Wstate-ManneG-20140228-SD002.pdf.

[155] *See Issuance of The Internet of Things: Privacy and Security in a Connected World Staff Report*, *supra* note 152, at 4.

cy" vote be disclosed on the first page of all reports or other documents containing recommendations.

Such a mechanism would effectively expand the set of options for which Commissioners could vote, enabling them to express subtler degrees of preference without constraining them, as now, into making the binary choice between approving or rejecting a recommendation *in toto*. In other words, while the cost of expressing disapproval today, in the form of a dissent from a report, may be too high in some cases (especially for Commissioners in the majority party), the cost of expressing disapproval for the sufficiency of analysis without vetoing an entire report would be much lower. Allowing such a vote, and publishing its results, would offer important information to the public. It would also increase the leverage of commissioners most concerned with ensuring that FTC recommendations are supported by sufficient rigor to influence the content and conclusions of FTC reports and similar documents.

In cases where the three-member majority feels the two-member minority's objections to analytical rigor are merely a pretense for objections to the recommendations themselves, the bill as we envision it would do nothing to stop the majority from issuing its recommendations anyway, of course; the "sufficiency" vote in this sense may sometimes be merely an expression of preference. Nonetheless, the majority Commissioners would likely be compelled to do more to explain why they believe the analysis included in support of a recommendation is sufficient, and why the minority is conflating its own policy views with the question of analytical sufficiency. These would also be valuable additions to the public's understanding of the basis for Commission recommendations

The virtue of our proposed approach is that it would further lower the bar for the Commission to do something it ought to do anyway: involve the Bureau of Economics in its decision-making.

RECOMMENDATION: Codify Congress's Commitment to Competition Advocacy

As we propose amending the RECS Act, consistent with the spirit with which we believe the bill is intended, BE would also have to be involved in any competition advocacy filings made by the FTC. Again, we believe this is all for the good. But it might, on the margin, discourage the FTC from issuing such filings in the first place — something we believe the FTC already does not do enough of. Thus, as discussed below, we recommend that Congress do more to encourage competition advocacy filings by the FTC.[156] At minimum, this means amending Section 6 to provide specific statutory authority for competition advocacy, something the FTC only vaguely divines from the Section today. As the text stands today, this authority is far from apparent, especially because the current Section 6 makes reference

[156] *See infra* note 87.

to "recommendations" only with respect to *Congress* in what we above refer to as Section 6(f)(ii).

Other Sources of Enforcement Authority (Guidelines, etc.)

The Solidifying Habitual & Institutional Explanations of Liability & Defenses (SHIELD) Act

Rep. Mike Pompeo's (R-KS) bill (H.R. 5118)[157] clarifies what is already black letter law: agency guidelines do not create any binding legal obligations, either upon regulated companies or the FTC. This means the FTC can bring enforcement actions outside the bounds of its Unfairness and Deception Policy Statements, its Unfair Methods of Competition Enforcement Policy Statement, and its regulations promulgated under other statutes enforced by the Commission (*e.g.*, the "Safeguards Rule," promulgated under the Gramm-Leach-Bliley Act)[158] unless Congress codifies the Statements in the statute. The only substantively operative provision of the bill is section (B), which provides that:

> Compliance with any guidelines, general statement of policy, or similar guidance issued by the Commission may be used as evidence of compliance with the provision of law under which the guidelines, general statement of policy, or guidance was issued.

This does not create a formal safe harbor; it merely allows companies targeted by the FTC to cite FTC's past guidance in their defense. This should be uncontroversial.

VALUE OF THE BILL: Increasing Legal Certainty and Decreasing the Coercive Regulatory Effect of the FTC's Soft Law

The bill would accomplish two primary goals. First, it would formally bar the FTC from doing something it has likely been doing in practice for some time: treating its own informal guidance as quasi-regulatory. To the extent that the Commission actually does so, it would effectively be circumventing the safeguards Congress imposed in 1980 upon the FTC's Section 5 rulemaking powers by amending the FTC Improvement Act of 1975 (commonly called "Magnuson-Moss").[159] But of course, for exactly this reason, the Commission would

---

[157] Solidifying Habitual and Institutional Explanations of Liability and Defenses Act, H.R. 5118, 114th Cong. (2016) [hereinafter SHIELD Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5118/text.

[158] Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

[159] The term Magnuson-Moss is inapt for two reasons. First, as former Chairman Muris explains, "Although within the Commission these procedures are uniformly referred to as 'Magnuson Moss,' in fact, the procedures are contained within Title II of the Magnuson Moss Warranty–Federal Trade Commission Improvement Act of 1975. Only Title I involved the Magnuson Moss Warranty Act…" *Statement of Timothy J. Muris*, *supra* note

(cont.)

never *admit* that this is what it is doing when its enforcement agenda just happens to line up with its previous recommendations.

More clear and more troubling is that, in the *LabMD* case, the Commission argued that the company, a small cancer testing lab, had committed an unfair trade practice sometime between 2006 and 2008 by failing to take "reasonable" measures to prevent the installation and operation of peer-to-peer file-sharing software on its network, which made patient billing information accessible to Tiversa, a company with specialized tools capable of scouring P2P networks for sensitive information. Crucial to the FTC's Complaint was its allegation that:

> Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.[160]

The Commission was referring, obliquely, to its 2005 report,[161] which offered this rather unhelpful suggestion to affected companies:

> Industry should decrease risks to consumers through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.

Not until January 2010 did the FTC issue "Peer-to-Peer File Sharing: A Guide for Business"[162] — about the same time, it appears, that the FTC undertook its investigation of LabMD. The SHIELD Act would clearly bar the FTC from pointing to its own past guidance as creating a legal trigger for liability. The Commission's assessment of "reasonableness" would have to be proven through other factors; indeed, since "reasonable" is found nowhere in Section 5 or even in the Unfairness Policy Statement, the Commission would have to prove the underlying elements of unfairness, without shortcutting this analysis by oblique reference to its own past reports.

A related concern is the Commission's application of rules promulgated in one context, in which they have binding authority, to other contexts in which they do not. The most striking example of this practice is the Commission's use of the Safeguards Rule, which "applies to the handling of customer information by all financial institutions over which the [FTC]

14, at 22, n. 44. Second, the safeguards at issue were adopted in 1980, not 1975, when "Mag-Moss" was passed.

[160] Complaint, In the Matter of LabMD, Inc., Docket No. 9357 at 4, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

[161] PEER-TO-PEER FILE-SHARING TECHNOLOGY, *supra* note 145.

[162] Fed. Trade, Comm'n, *Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business.

has jurisdiction,"[163] to define unfair data security practices, and the remedies applied by the FTC in consent decrees, outside the financial sector. Although the Safeguards Rule has regulatory authority for financial institutions, its authority is no different than informal guidance (or recommended "best practices") the Commission offers for everyone else. Nevertheless, the Commission has imposed remedies virtually identical to the Safeguards Rule in nearly every data security consent order into which it has entered.

> [T]he majority of the FTC's [data security] cases, regardless of cause of action or facts, impose the same remedy: the set of security standards laid out in the FTC's Safeguards Rule. Most notably, this is true regardless of whether the respondents were financial institutions (to which the Safeguards Rule directly applies) or not (to which the Rule has no direct application), and regardless of whether the claim is generally one of deception or unfairness.[164]

Second, the SHIELD Act would allow companies to raise their compliance with FTC guidance as part of their defense. This would, at a minimum, help encourage companies to resist settling legally questionable or analytically unsupported enforcement actions.

RECOMMENDATION: Clarify that Consent Decrees, Reports, and FTC Best Practices are not Binding

We propose expanding the bill's language slightly to ensure that it achieves its intended goal:

> No guidelines, general statements of policy, ***consent decrees, settlements, reports, recommended best practices***, or similar guidance issued by the Commission shall confer any right.

As should be clear by now, these other forms of soft law are the most important aspects of the FTC's discretionary model, especially given the paucity of policy statements (building upon the three major ones, such as on materiality, for example) or issue-specific "Guides."

Specifically, the Commission regularly applies its recommended best practices (grouped under catchphrases like "privacy by design" and "security by design") as mandatory company-specific regulations in consent decrees that are themselves applied, in cookie-cutter fashion, across enforcement actions brought against companies that differ greatly in their circumstances, and regardless of the nature or extent of the injury or the specific facts of their case.

Second, the *LabMD* case provides at least one clear example wherein the FTC has treated its own previous reports, making vague recommendations about the need for better industry data security practices (regarding peer-to-peer file-sharing), as a critical part of the trigger for

---

[163] 16 C.F.R. § 314.1(b).

[164] Manne & Sperry, *supra* note 52, at 20.

legal liability.[165] We suspect this is the tip of the iceberg — that the FTC in fact does this kind of thing quite often, but usually does not have to admit it, because it is able to settle cases without revealing its legal arguments. Only in the *LabMD* case (one of the first (of two) data security cases to be litigated after more than a decade of FTC consent decrees in this area) did the Commission have to make the connection between its previous "recommendations" and its application of Section 5. Even here, in its *LabMD* Complaint, it should be noted, the Commission did not specifically cite its 2005 P2P file-sharing report, but instead vaguely alluded to it — suggesting that even FTC staff were wary of revealing this connection.

RECOMMENDATION: Specify When a Defendant May Raise Evidence of Its Compliance with FTC Guidance

The bill does not currently specify *when* in the enforcement process evidence of compliance may be cited. It is important that a defendant be able to raise a compliance defense as early as possible. Without such an opportunity, the Commission can drag out an investigation that should have been terminated early, as when the subject of the investigation acted in good faith reliance upon the Commission's own statements. Ideally, this would occur during motions to quash CIDs.

Further, it would help if the FTC amended its rule on such motions, 16 C.F.R. § 2.10, to specify that this defense could be raised at part of a motion to quash. And, as we noted above,[166] it is critical that these challenges be permitted to remain confidential, as many companies may choose to avoid the risk the public exposure that comes with challenging CIDs.

At a minimum, the defendant should be able to raise this defense in a way that is communicated to Commissioners *before* the Commission's vote on whether to issue a complaint.

RECOMMENDATION: Encourage the FTC to Issue More Policy Statements & Guides

As the proposed SHIELD Act reflects, while there is some risk of ossification from over-reliance on *ex ante* guidelines and policy statements, the absence of such guidance documents can leave consumers and economic actors with insufficient notice of FTC enforcement principles and practices. Absent meaningful constraints on the Commission's discretionary authority, the costs of over-enforcement may be as great or greater than the costs of over-regulation. For these reasons, the bill should require the FTC to issue substantive

---

[165] *See supra* note 66 and note 161.

[166] *See supra* at 46.

guidelines, allow private parties to petition the FTC to issue guidelines, or allow a single Commissioner to force the issue.

A good place to start would be privacy regulation, where the Commission has issued no meaningful guides.[167] The Commission has done better on data security, with guides, for example, on photocopier data security (2010),[168] P2P software (2010),[169] and mobile app security (2013).[170] But none of these, and even the particularly thorough "Start with Security: A Guide for Business" (2015),[171] does the kind of thing the various antitrust guidelines do: expand upon the *analytical framework* by which the Commission determines how much security is enough. This must be grounded in the component elements of Section 5, not the Commission's policy agenda or technical expertise.

More important than issue-specific guides would be guidance one step up the Doctrinal Pyramid, explaining how concepts like materiality, weighing injury with benefits, and measuring reasonable avoidability will be measured.[172] Such a document would greatly enhance the value of issue-specific guides by allowing regulated companies to understand not just what the Commission might demand in the future, but the doctrinal legal basis for doing so.

Remedies

Appropriate Tailoring of Remedies

No Bill Proposed

The FTC has, perhaps predictably, also pushed the envelope with regard to the sorts of remedies it seeks against a broader category of targets. Initially, the Commission was given authority to pursue permanent injunctions under Section 13(b) as part of its ongoing mission to curb outright fraud.[173] Over time, however, the FTC has expanded its use of Section 13(b)

---

[167] See, e.g., Fed. Trade Comm'n, *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks* (Dec. 2012), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor

[168] Fed. Trade Comm'n, *Copier Data Security: A Guide for Businesses* (Nov. 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/copier-data-security-guide-businesses

[169] *Peer-to-Peer File Sharing: A Guide for Business*, *supra* note 162.

[170] Fed. Trade Comm'n, *Mobile App Developers: Start with Security* (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security

[171] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (Jun. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[172] *See supra* note 12.

[173] *See generally* Beales & Muris, *supra* note 21.

in order to target companies that engage in conduct that implicates issues from substantiation claims to product design — all far from fraudulent territory.[174]

For instance, Apple, Google, and Amazon have all been targets of the Commission for issues related to the design and function of their respective mobile app stores.[175] Amazon, one of the rare parties to proceed to full litigation on a Section 5 unfairness case, recently lost a summary judgment motion on a claim that its in-app purchasing system permitted children to make in-app purchases without parental "informed consent," thus engaging in an "unfair practice."[176] As part of its case the Commission sought a permanent injunction under Section 13(b) against Amazon on the basis of the Commission's claim that it was "likely to continue to injure consumers, reap unjust enrichment, and harm the public interest."[177]

This practice, called "fencing-in,"[178] may be appropriate for the inveterate fraudsters — against whom it is authorized under Section 19 of the Act:

> If the Commission satisfies the court that the act or practice to which the cease and desist order relates is **one which a reasonable man would have known under the circumstances was dishonest or fraudulent**, the court may grant… such relief as the court finds necessary.[179]

The FTC — in the past — indeed viewed Section 13(b) as a tool to police clearly fraudulent practices. "Consistent with the limitations in Section 19, the agency used Section 13(b) for a narrow class of cases involving fraud, near fraud, or worthless products."[180] Meanwhile, courts, for their part, "blessed this limited expansion of FTC authority," and still see the appropriate scope of Section 13(b) as a limited one.

---

[174] *Id.* at 4.

[175] *See* Geoffrey A. Manne, *Federal Intrusion: Too Many Apps for That*, WALL STR. J. (Sep. 16, 2014), http://www.wsj.com/articles/geoffrey-manne-federal-intrusion-too-many-apps-for-that-1410908397.

[176] Fed. Trade Comm'n v. Amazon.com, Inc., Case No. C14-1038-JCC, slip op. at 10 (W.D. Wash 2016), available at https://www.ftc.gov/system/files/documents/cases/160427amazonorder.pdf.

[177] *Id.* at 10.

[178] *See, e.g.*, Federal Trade Commission V. RCA Credit Services, LLC, Case No. 8:08-CV-2062-T-27AEP. (M.D. Fla. Jul 21, 2010) at 20 ("Courts also have discretion to include 'fencing-in' provisions that extend beyond the specific violations at issue in the case to prevent Defendants from engaging in similar deceptive practices in the future.").

[179] 15 U.S.C. § 57(b)-(a)(2) and -(b).

[180] Beales & Muris, *supra* note 21, at 22.

But the argument for extending fencing-in beyond the fraud context is extremely weak. Nevertheless, the FTC has more recently, as in the *Amazon* case, sought to use 13(b) against legitimate companies, dramatically expanding its scope — and its *in terrorem* effect.[181]

> Such broad "fencing in" relief (imposition of behavioral requirements that are more extensive than required [in order] to avoid future violations) goes well beyond prior FTC practice and may be aimed at "encouraging" other firms in similar industries to adopt costly new testing.[182]

Effectively, from the Commission's perspective, Amazon — with its app store that satisfied the needs of a huge number of consumers — was legally equivalent to "defendants engaged in continuous, fraudulent practices [who] were deemed likely to reoffend based on the 'systemic nature' of their misrepresentations."[183] This could not have been what Congress intended.

The courts, when they are presented with the opportunity to review this approach (as they sometimes are in Deception cases and as they virtually never are in Unfairness cases, given the lack of litigation) have been less than receptive. Although Amazon lost its motion for summary judgment, it prevailed on the question of whether Section 13(b) presented an appropriate remedy for its alleged infractions.

> While permanent injunctions are often awarded in cases where liability under the FTC Act is determined, Amazon correctly distinguishes those cases from the facts of this case… [C]ases in which a permanent injunction has been entered involved deceptive, ongoing practices.[184]

The court properly noted that it was incumbent upon the Commission to "establish, with evidence, a cognizable danger of a recurring violation."[185]

Similarly, in *FTC v. RCA Credit* (a Deception case), the court rejected the FTC's use of 13(b) — in that case, accepting the permanent injunction but questioning the expansion of its scope:

> The undisputed facts demonstrate that this is a proper case for permanent injunctive relief. However, the Court will defer ruling on the appropriate scope of an injunction (including whether, as the FTC requests, the injunction should include a

---

[181] *Id.* at 4 ("The FTC now threatens to expand the use of the Section 13(b) program beyond fraud cases, suggesting that it may use Section 13(b) to seek consumer redress even against legitimate companies.").

[182] Alden Abbott, *Time to Reform FTC Advertising Regulation*, Heritage Foundation Legal Memorandum #140 on Regulation (Oct. 29, 2014), *available at* http://www.heritage.org/research/reports/2014/10/time-to-reform-ftc-advertising-regulation#_ftnref21.

[183] Amazon case at 11.

[184] Amazon case at 11.

[185] *Id.* at 11.

> broad fencing-in provision enjoining misrepresentations of material fact in connection with the sale of any goods and services) until after hearing evidence on the issue.[186]

The reluctance of some courts to abet the FTC's expansion of its use of fencing-in remedies to reach legitimate companies is reassuring — and affirms our belief as to what Congress intended in Section 13(b). Unfortunately, however, most parties do not proceed to ruinously expensive litigation with the Commission, and will accede to the demands of a consent order. This creates undue costs of both the first order (companies agreeing to remedies that are larger or more invasive than what a court would impose) and the second order (the systemic cost of companies settling cases they might otherwise litigate, all regulated entities losing the benefit of litigation, and the FTC having to do less rigorous analysis).

The FTC's ability to threaten a permanent injunction, or to dramatically extend its scope beyond the practices at issue in a case, gives parties an inefficiently large incentive to settle in order to avoid the risk of the more draconian remedy. But, in doing so, parties end up opting in to consent orders that allow the FTC to evade any judicially enforced limits on the remedies it imposes, which is what the Commission *really* wants. Whatever the benefits to the agency from permanent injunctions, it arguably receives even more benefit from the ability to impose more detailed behavioral remedies than a court might permit (and to do so in the context of a consent order, the violation of which is subject to the lower burden of proving contempt rather than an initial violation).

The Commission's general resistance to constraints upon its remedial discretion was aptly illustrated by its abrupt revocation, in 2012,[187] of its 2003 Policy Statement On Monetary Equitable Remedies in Competition Cases (commonly called the Disgorgement Policy Statement).[188] As Commissioner Ohlhausen noted in her dissent from the withdrawal of the policy:

> Rescinding the bipartisan Policy Statement signals that the Commission will be seeking disgorgement in circumstances in which the three-part test heretofore utilized under the Statement is not met, such as where the alleged antitrust violation

---

[186] RCA Credit case at 24.

[187] Fed. Trade Comm'n, *FTC Withdraws Agency's Policy Statement on Monetary Remedies in Competition Cases; Will Rely on Existing Law* (Jul. 31, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies.

[188] Fed. Trade Comm'n, Policy Statement On Monetary Equitable Remedies — Including in Particular Disgorgement and Restitution, in FEDERAL TRADE COMMISSION COMPETITION CASES ADDRESSING VIOLATIONS OF THE FTC ACT, THE CLAYTON ACT, OR THE HART-SCOTT-RODINO ACT (2003), *available at* https://www.ftc.gov/public-statements/2003/07/policy-statement-monetary-equitable-remedies-including-particular.

> is not clear or where other remedies would be sufficient to address the violation.[189]

Not only does this mean that parties in general are more likely to settle, but it also means that parties that are facing novel, untested antitrust theories are more likely to settle. This allows the Commission to expand its antitrust enforcement authority beyond judicially recognized conduct without risk of reversal by the courts.

Section 13(b) and the Commission's disgorgement powers represent tremendous weapons to wield over the heads of investigative targets. Their expanding use to impose expansive or draconian remedies in cases involving non-fraudulent, legitimate companies and questionable legal theories is extremely troubling. Not only is this bad policy, it is also inconsistent with the spirit of the FTC Act, which was designed to find and punish actively fraudulent conduct, and to deter anticompetitive behavior that is not countervailed by pro-consumer benefits. But most of all, this gives the FTC greater ability to coerce companies that might otherwise litigate into settlements, pushing us further away from the Evolutionary Model and towards the Discretionary Model.

To correct these problems, at least two things should be done:

RECOMMENDATION: Limit Injunctions to the "Proper Cases" Intended by Congress

First, the Commission's use of Section 13(b) remedies should be reevaluated in light of the law's original purpose:

> [O]ne class of cases clearly improper for awarding redress under Section 13(b): traditional substantiation cases, which typically involve established businesses selling products with substantial value beyond the claims at issue and disputes over scientific details with well-regarded experts on both sides of the issue. In such cases, the defendant would not have known ex ante that its conduct was "dishonest or fraudulent." Limiting the availability of consumer redress under Section 13(b) to cases consistent with the Section 19 standard strikes the balance Congress thought necessary and ensures that the FTC's actions benefit those that it is their mission to protect: the general public.[190]

---

[189] Dissenting Statement of Commissioner Maureen K. Ohlhausen, *Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases* (Jul. 31, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120731ohlhausenstatement.pdf.

[190] Beales & Muris, *Striking the Proper Balance*, *supra* note 21, at 6.

[190] 15 U.S.C. § 57(b)-(a)(2) and -(b).

[190] Beales & Muris, *Striking the Proper Balance*, *supra* note 21, at 6–7.

This same logic applies to a host of other types of cases, as well, including the Commission's recent product design cases.[191] Thus the tailoring of the Commission's Section 13(b) powers should not stop merely with substantiation cases, but should extend, as a general principle, to any party that had not intentionally or recklessly engaged in conduct it should have known was dishonest or fraudulent. As Josh Wright noted in his dissent in the Apple product design case:

> The economic consequences of the allegedly unfair act or practice in this case — a product design decision that benefits some consumers and harms others — also differ significantly from those in the Commission's previous unfairness cases.
>
> The Commission commonly brings unfairness cases alleging failure to obtain express informed consent. These cases invariably involve conduct where the defendant has intentionally obscured the fact that consumers would be billed. Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud — the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items. Under this scenario, the allegedly unfair act or practice injures consumers and does not provide economic value to consumers or competition. In such cases, the requirement to provide adequate disclosure itself does not cause significant harmful effects and can be satisfied at low cost.
>
> However, the particular facts of this case differ in several respects from the above scenario.[192]

The same logic that undergirds former Commissioner Wright's objection to the majority's aggressive application of the UPS in *Apple* applies equally to the aggressive 13(b) remedies sought in similar cases.

RECOMMENDATION: Narrow Overly Broad "Fencing-in" Remedies

Similarly, the imposition of unreasonable behavioral demands — "fencing-in" of conduct beyond that at issue in the case — upon parties subject to FTC enforcement is problematic.

---

[191] Fed. Trade Comm'n, *FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges* (Jul. 10, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars; In the Matter of Apple Inc., FTC File No 112 3108, https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc (2014); Fed. Trade Comm'n, *Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges* (Sept. 4, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it.

[192] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 3 (Jan. 15, 2014), *available at* https://goo.gl/0RCC9E.

.

For instance, in *Fanning v. FTC*, the Commission imposed upon defendant John Fanning a requirement that the First Circuit characterized as "not reasonably related to [the alleged] violation."[193] In 2009, Fanning founded jerk.com, a social networking website that controversially enabled users to nominate certain persons to be "jerks."[194] In issuing a variety of challenges to jerk.com's business practices — including an alleged failure of the site to facilitate paid customers' removal of negative information — the Commission additionally applied a "compliance monitoring" provision aimed directly at Fanning.[195] This provision required that Fanning "notify the Commission of… his affiliation with any new business or employment," and submit information including the new business's "address and telephone number and a description of the nature of the business" for a period of ten years.[196] Under the Commission's cease and desist order, it did not matter whether Fanning engaged in reputation work, or started social media sites, or not — the requirement applied regardless of what type of work Fanning did and for whom he did it.[197]

The First Circuit rebuked the Commission on this point:

> When asked at oral argument, the Commission conceded that this provision would ostensibly require Fanning to report if he was a waiter at a restaurant. The only explanation offered by the Commission for this breadth is that it has traditionally required such reporting.[198]

Moreover, the Commission cited a string of district court cases upholding similar provisions which the court characterized as "almost entirely bereft of analysis that might explain the rationale for such a requirement."[199] While it is encouraging that the First Circuit saw fit to rein in the Commission, it is also apparent that the FTC frequently receives an extraordinary degree of deference from district courts, even when creating punitive provisions that bear little or no connection to challenged subject matter.

In order to deter the Commission from taking advantage of this frequent judicial deference by imposing such disconnected "fencing-in" remedies in non-fraud cases — which, of course, is compounded by the fact that most cases are never reviewed by courts at all — Congress should consider imposing some sort of minimal requirement that provisions in

---

[193] Fanning v. Fed. Trade Comm'n, FTC File No. 15-1520, slip op. at 13 (May 9, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/051816jerkopinion.pdf.

[194] *Id.* at 2-3.

[195] *Id.* at 21-22.

[196] *Id.* at 22.

[197] Final Order, Fanning v. Fed. Trade Comm'n, FTC File No. 15-1520 (March 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150325jerkorder.pdf

[198] *Id.* at 23-24.

[199] *Id.* at 24.

proposed orders and consent decrees be (i) reasonably related to challenged behavior, and (ii) no more onerous than necessary to correct or prevent the challenged violation.

This reform is also important to minimizing the daisy-chaining of consent decrees discussed in the next Section.[200] As we note there, the ability of the Commission to bring a second enforcement action not premised on Section 5, but rather on the terms of a consent decree that is vaguely related to the challenged conduct creates several problems. The Commission's ability to do this is magnified if the initial consent order already contains provisions that reach a broad range of conduct or that include a host of difficult conduct remedies that the company may even inadvertently violate.

RECOMMENDATION: Revive the 2003 Disgorgement Policy

Second, Congress should consider requiring the Commission to return to its previous disgorgement policy, or to propose targeted amendments to it. At a minimum, the Commission should be required to perform *some* process to examine the issue and take public comment on it. As Commissioner Ohlhausen noted in her dissent, objecting to the vote to rescind the Policy Statement:

> I am troubled by the seeming lack of deliberation that has accompanied the withdrawal of the Policy Statement. Notably, the Commission sought public comment on a draft of the Policy Statement before it was adopted. That public comment process was not pursued in connection with the withdrawal of the statement. I believe there should have been more internal deliberation and likely public input before the Commission withdrew a policy statement that appears to have served this agency well over the past nine years.[201]

Consent Decree Duration & Scope

The Technological Innovation through Modernizing Enforcement (TIME) Act

Subcommittee Chairman Rep. Michael C. Burgess, M.D.'s (R-TX) bill (H.R. 5093)[202] would, in non-fraud cases, limit FTC consent orders to eight years — instead of the 20 years the FTC usually imposes. If the term runs five years or more, the FTC must reassess the decree after five years under the same factors required for setting the length of the consent decree from the outset:

---

[200] *See infra* at 76.

[201] *Id.* at 2.

[202] The Technological Innovation through Modernizing Enforcement Act, H.R. 5118, 114th Cong. (2016) [hereinafter TIME Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5093/text.

1. The impact of technological progress on the continuing relevance of the consent order.
2. Whether there is reason to believe that the entity would engage in activities that violate this section without the consent order 8 years after the consent order is entered into by the Commission.

Shortening the length of consent decrees will do much to address the abuse of consent decrees, but it will not fix the underlying problems, as we discuss below.

VALUE OF THE BILL: Reducing the Abuse of Consent Decrees as *De Facto* Regulations

This reform is critical to reducing the FTC's use of consent decrees as effectively regulatory tools. It is entire commonplace for the FTC to impose the same twenty-year consent decree term and the same conditions (drawn from its quasi-regulatory reports) on every company, regardless of the facts of the case, the size of the company etc. Limiting the duration of consent decrees would not entirely stop abuse of consent decrees as a way to circumvent Section 5 rulemaking safeguards (because each consent decree is effectively a mini-rulemaking, which implements the FTC's pre-determined policy agenda), but it would at least limit the damage, and clear overly broad consent decrees more quickly.

The bill would also make it less likely that the FTC could daisy-chain additional enforcement actions — that is, bring a second enforcement action not premised on Section 5 (and therefore not even paying lip service to its requirements) but on the terms of a consent decree that is only vaguely related to the subsequent conduct. Such daisy-chaining has allowed enormous leverage in forcing settlements, since the FTC Act gives the Commission civil penalty authority only for violations of consent decrees (and rules), not Section 5 itself. Thus, the FTC gains the sledgehammer of potentially substantial monetary fines the second time around. It also allows the FTC to further extend the term of the consent decree beyond the initial 20 years — and potentially keep a company operating under a consent decree forever.

This is essentially what the FTC did to Google. First, in 2011, the FTC and Google settled charges that Google had committed an unfair trade practice in 2010 in by opting Gmail users into certain features of its new (and later discontinued) Buzz social network.[203] A year later, the FTC imposed a $22.5 million penalty against Google in settling charges that Google had violated the 2011 consent decree by misleading consumers by, essentially, failing to update an online help page that told users of Apple's Safari browser that they did not need to take further action to avoid being tracked, after a technical change made *by Apple*

[203] Fed. Trade Comm'n, *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Networ*k (Mar. 30, 2011), available at https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

had rendered this statement untrue.[204] The FTC's Press Release boasted "Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order."[205] The case raised major questions about the way the FTC understood its deception authority,[206] none of which were dismissed because (a) Google, already being under the FTC's thumb and facing a potentially even-larger monetary penalty, was eager to settle the case, and (b) the FTC technically did not have to prove the normal elements of deception, such as the materiality of a help page seen by a tiny number of users, because it was enforcing the consent decree, not Section 5.

Perhaps most disconcertingly, the Commission's 2012 action against Google had precious little to do with the conduct that gave rise to its 2011 consent order. To be sure, the 2011 order was written in the broadest possible terms, arguably covering nearly every conceivable aspect of Google's business. But this just underscores the regulation-like nature of the Commission's consent orders, as well as the FTC's propensity to treat cases with dissimilar facts and dissimilar circumstances essentially the same. While that kind of result might be expected of a regulatory regime, it is inconsistent with the idea of case-by-case adjudication, which also puts paid to the idea that of a "common law of data security consent decrees":

> In this sense the FTC's data security settlements aren't an evolving common law — they are a static statement of "reasonable" practices, repeated about 55 times over the years and applied to a wide enough array of circumstances that it is reasonable to assume that they apply to *all* circumstances. This is consistency. But it isn't the common law. The common law requires consistency of application — a consistent theory of liability, which, given different circumstances, means *inconsistent* results. Instead, here we have consistent results which, given inconsistent facts, means [] *in*consistency of application.[207]

RECOMMENDATION: Allow Petitions for Appeal of Mooted Consent Decrees

Noticeably *not* addressed by this bill is the situation in which the FTC has found a company in violation of Section 5 for some practice (and imposed a consent decree for the violation), then lost in court on essentially the same doctrinal point. At a minimum, part of the reassessment of any consent decree should include assessing whether court decisions have called into question whether the original allegation actually violated Section 5. Ideally, the bill

---

[204] Fed. Trade Comm'n, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012) available at https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[205] *Id.*

[206] *See, e.g.*, *FTC's Google Settlement a Pyrrhic Victory for Privacy and the Rule of Law*, International Center for Law & Economics (Aug. 9, 2012), *available at* http://www.laweconcenter.org/component/content/article/84-ftcs-google-settlement-a-pyrrhic-victory-for-privacy-and-the-rule-of-law.html.

[207] Manne & Sperry, *supra* note 52, at 13.

should also include a procedure by which the company subject to a consent decree could petition for review of its consent decree on these grounds.

Such an amendment should not be controversial, given that the FTC so rarely (if ever) litigates its consumer protection cases.

Other Process Issues

Open Investigations

The Start Taking Action on Lingering Liabilities (STALL) Act

Rep. Susan Brooks' (R-IN) bill (H.R. 5097)[208] would automatically terminate investigations six months after the last communication from the FTC. Commission staff can keep an investigation alive either by sending a new communication to the target or the Commissioners can vote to keep the investigation open (without alerting the target). Current FTC rules allow the staff to inform targets that their investigation has ended, but does *not* require them to do so.[209]

VALUE OF THE BILL: Good Housekeeping, Reduces *In Terrorem* Effects of Lingering Investigations

This should be among the least controversial of the pending bills. It is simply a good housekeeping measure, ensuring that companies will not be left hanging in limbo after initial investigation-related communications from the FTC.

Closing open investigations could have several benefits.

First, in some circumstances, publicly traded companies may conclude that they are required to disclose the FTC's inquiry in their SEC filings.[210] That, in turn, can spark a media frenzy that could be as damaging to the company as whatever terms the FTC might impose in a consent decree — or at least seem to be less costly to managers who are more incentivized to care about the immediate performance of the company than the hassle of being sub-

---

[208] Start Taking Action on Lingering Liabilities Act, H.R. 5097, 114th Cong. (2016) [hereinafter STALL Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5097/text.

[209] Fed. Trade Comm'n, *Operating Manual: Chapter 3: Investigations*, 46 (last visited May 20, 2016), *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch03investigations_0.pdf (providing, in .3.7.4.5, that "[i]n investigations which have been approved by Bureau Directors, closing letters are ordinarily sent to both the applicant and the proposed respondent, with copies to their attorneys, if any[,]" but not requiring such letters in any case).

[210] *See, e.g.*, Deborah S. Birnbach, *Do You Have to Disclose a Government Investigation?*, *supra* note 99.

ject to an FTC consent decree for the next 20 years.[211] Making such disclosures can be particularly problematic if management intends to shop the company around for acquisition.

Presumably, a company that feels compelled to disclose an investigation in an SEC filling would, today, *eventually* feel justified in modifying the disclosure to indicate its belief that the investigation has concluded, given a long enough period of silence from the Commission. But this could take years, during which time the "lingering liability" could continue to damage the company. The bill (if it includes our proposed amendment, below) would give companies a clear indication whether or not they can modify their quarterly disclosures and inform shareholders and the general public that an investigation has concluded.

Second, giving subject companies repose after six months of silence from the FTC would allow management to focus on running their businesses. This could be especially critical for small companies.

Third, giving companies greater certainty in this way would reduce the leverage that staff may have to coerce companies into settling cases that might otherwise not be brought at all, or that companies might litigate. That means, in the first instance, moving closer to the optimal number of cases settled and, in the second instance, increasing the potential for litigation where it is warranted, which benefits everyone by allowing "the underlying criteria [of Section 5] to evolve and develop over time" through "judicial review," as the Unfairness Policy Statement explicitly intends.[212]

Fourth, holding target companies *in terrorem* may have other indirect costs besides driving companies to settle questionable cases. The longer an investigation lingers, or the longer it *could* linger (before the company can safely assume it is over), the more likely the company is to treat the FTC's "recommended" best practices as effectively mandatory, regulatory requirements. This regulation-by-terror is impossible to quantify, but it is a very real concern. To the extent it happens, it contributes to transforming the FTC's "inquisitorial powers" into a tool by which the FTC may treat its workshops and reports as de facto rulemakings, thus at least partially circumventing the Section 5 rulemaking safeguards.

Finally, the bill makes it harder for FTC staff to circumvent Bureau Director oversight — and thus avoid any possibility of alerting Commissioners. Current FTC rules allow an Initial Phase Investigation to be conducted for up to 100 hours of staff time, after which Staff must

---

[211] Notably, this also includes the potential for the FTC to bring additional enforcement actions premised on violating the terms of the consent decree, however attenuated the subsequent enforcement action might be, which is even easier than bringing an enforcement action premised directly on Section 5 (in that the FTC need not even purport to satisfy the requirements of Section 5). *See e.g.*, United States v. Google, Inc., Case 5:12-cv-04177-HRL (N.D.Ca. 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[212] UPS, *supra* note 9.

draft a memo and obtain approval from the Bureau Director to continue the investigation.[213] Today, the staff may be able to shoehorn a new investigation into an old investigation for which they have already received Director approval, thus avoiding or forestalling having to seek new approval from the Bureau Director. One can imagine that this would be particularly appealing if the Commission's majority — and thus also its Bureau Directors, who are appointed by the Chairman — has switched parties. This shoehorning may be very easy to do given the breadth of the FTC's investigations: one inquiry about questionable data security could very easily morph into another, potentially years later. The proposed bill would reduce this possibility by reducing the menu of available investigations from which staff could pick and choose. In other words, it would help to draw lines between old investigations and new ones. While this should not be a significant burden for the Staff, it should help to ensure that other internal decisionmaking safeguards are respected.

RECOMMENDATION: Bar Secret Votes as a Means of Evading the Bill

As drafted, the bill would allow the Commission to take a (non-public) vote to keep an investigation alive without the subject receiving additional communications. We can think of no reason to permit the Commission to hide the existence of a continuing investigation from its subject, however. In fact, although doing so requires a small price (an affirmative vote of the Commission), the price is so small that it is reasonable to expect that the exception would subsume the rule, and permit the Commission to evade the overall benefits of the proposed bill. Thus, we suggest amending section (2)(B) of the proposed bill, which authorizes an investigation to continue if "the Commission votes to extend the covered investigation before the expiration of such period,"[214] to also require the Commission to send a communication to the subject informing it of the vote. This would add no appreciable cost to the Commission's ability to extend an investigation, but, unlike a non-public vote, it ensures that the subject is made aware of the extension.

This amendment would have the benefit of allowing the subject's management to take *true* repose, knowing that an investigation had truly ended. Only then, for instance, would many managers feel comfortable revising a public securities disclosure about the company's lingering potential liability. In short, this would allow companies to clear their good names and get on with the business of serving consumers.

---

[213] Operating Manual at 9, § 3.2.1.1.

[214] STALL Act, *supra* note 208.

Commissioner Meetings

The Freeing Responsible & Effective Exchanges (FREE) Act

Rep. Pete Olson's (R-TX) bill (HR 5116)[215] would allow a bipartisan quorum of FTC Commissioners to meet confidentially under certain circumstances: no vote or agency action may be taken, the meeting must be FTC staff only, with a lawyer from the Office of General Counsel present, and the meeting must be disclosed publicly online. This would greatly empower other Commissioners by allowing them to meet with each other and with Commission staff — potentially without the Chairman, or without the Chairman having organized the meeting.

The bill does essentially the same thing as the FCC Process Reform Act of 2015 (H.R. 2583), which was so uncontroversial that it passed the House on a voice vote in November 2015.[216] Both bills would, for the affected agency, undo an unintended consequence of the Government in the Sunshine Act of 1976. That well-intentioned effort to bring transparency to agency decision-making in the aftermath of the Watergate scandal has the had the perverse result of undermining the very purpose of multi-member commissions.

VALUE OF THE BILL: Restoring the Collegiality of the FTC

The Sunshine Act calls multi-member commissions "collegial bod[ies],"[217] but the effect of the law has been to greatly contribute to the rise of the Imperial Chairmanship, because the law not only requires that "disposing of" (*i.e.*, voting on) major items (*e.g.*, rulemakings or enforcement actions) be conducted in public meetings (organized by the Chairman), it also bars Commissioners from "jointly conduct[ing]… agency business" except under the Act's tight rules. In effect, this makes it difficult for other Commissioners to coordinate without the Chairman.

The bill would continue to require that any "vote or any other agency action" be taken at meetings held under the Sunshine Act. This would ensure that the FTC generally continues to operate in full public view and according to valid process.

But the bill would allow Commissioners to meet privately, potentially without the Chairman present.

---

[215] The Freeing Responsible and Effective Exchanges Act, H.R. 5116, 114th Cong. (2016) [hereinafter FREE Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5116/text.

[216] Federal Communications Commission Process Reform Act of 2015, H.R. 2583, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/2583/actions

[217] 5 U.S.C. § 552b(a)(1) & (3).

The benefits of such meetings are self-evident. They would encourage collegiality and facilitate bipartisan discussions, leading to a more open and inclusive process. They would also provide opportunities for minority commissioners to be apprised earlier in the process when the Commission is considering various actions, from investigations to issuing consent decrees.

The fact that the Energy & Commerce Committee has already vetted these reforms for the FCC, and that the full House has already voted for them as part of a larger FCC reform package, should make passage of this bill straightforward.

RECOMMENDATION: Ensure that Two of Three Commissioners Can Meet

As amended by the bill, 15 U.S.C. § 552b(d)(2)(A) would require that the group consist of at least three or more Commissioners. This would have the perverse result of rendering the bill useless at present, when the Commission has only three Commissioners — because all three would have to be present for a meeting. We recommend simply striking this subsection, so that, on a three-member commission, the Democrat and Republican commissioners can meet without the Chairman.

Part III Litigation

Numerous commentators have raised serious questions about the FTC's use of adjudication under Part III of the FTC's Rules. Commissioner Wright put it best in a 2015 speech:

> Perhaps the most obvious evidence of abuse of process is the fact that over the past two decades, the Commission has almost exclusively ruled in favor of FTC staff. That is, when the ALJ agrees with FTC staff in their role as Complaint Counsel, the Commission affirms liability essentially without fail; when the administrative law judge dares to disagree with FTC staff, the Commission almost universally reverses and finds liability. Justice Potter Stewart's observation that the only consistency in Section 7 of the Clayton Act in the 1960s was that "the Government always wins" applies with even greater force to modern FTC administrative adjudication.
>
> Occasionally, there are attempts to defend the FTC's perfect win rate in administrative adjudication by attributing the Commission's superior expertise at choosing winning cases. And don't get me wrong – I agree the agency is pretty good at picking cases. But **a 100% win rate is not pretty good; Michael Jordan was better than pretty good and made about 83.5% of his free throws during his career, and that was with nobody defending him. One hundred percent isn't Michael Jordan good; it is Michael Jordan in the cartoon movie "Space Jam" dunking from half-court good.** Besides being a facially implausible defense – the data also show appeals courts reverse Commission decisions at four times the rate of feder-

> al district court judges in antitrust cases suggests otherwise. This is difficult to square with the case-selection theory of the FTC's record in administrative adjudication.[218]

Former FTC Chairman Terry Calvani provides an apt summary of empirical research on the FTC's perfect win rate.[219] He notes FTC practitioner David Balto's study of eighteen years of FTC litigation, in which "the FTC has never found for the respondent and has reversed all ALJ decisions finding for the respondent."[220] Balto concluded "there appears to be a lack of impartiality by the Commission that really undermines the credibility of the process, and I think that makes it more difficult for the FTC to effectively litigate tough cases and get the court of appeals to support [its] decisions going forward."[221]

We recommend that Congress consider one of two structural reforms.

RECOMMENDATION: Separate the FTC's Enforcement & Adjudicatory Functions

Former Chairman Calvani proposes that

> the FTC be reorganized to separate the prosecutorial and adjudicatory functions. The former would be vested in a director of enforcement appointed by and serving at the pleasure of the president. Commissioners would hear the cases brought before the agency. This model is not alien to American administrative law and independent agencies. Labor complaints are evaluated and issued by National Labor Relations Board ("NLRB") regional directors. Administrative hearings are held before ALJs, and appeals from the ALJs are vested in the NLRB. Similarly, the Securities and Exchange Commission's ("SEC's") prosecutorial functions are vested in the Division of Enforcement while administrative hearings are held before ALJs and appeals are vested in the SEC.
>
> This change in organization would eliminate the existence or perception of unfairness associated with the same commissioners participating in both the decision to initiate a case and in its ultimate resolution. It would also make the deci-

---

[218] Joshua D. Wright, Commissioner, Fed. Trade Comm'n, *Remarks at the Global Antitrust Institute Invitational Moot Court Competition*,16-17 (Feb. 21, 2015) (emphasis added), *available at* https://www.ftc.gov/system/files/documents/public_statements/626231/150221judgingantitrust-1.pdf.

[219] Terry Calvani & Angela M. Diveley, *The FTC At 100: A Modest Proposal for Change*, 21 GEO. MASON L. REV. 1169, 1178-82 (2014).

[220] *Id.* at 1179 (quoting David A. Balto, *The FTC at a Crossroads: Can It Be Both Prosecutor and Judge?*, LEGAL BACKGROUNDER (Wash. Legal Found.) (Apr. 23, 2013), 1).

[221] Wash. Lgl Found., *FTC's Administrative Litigation Process: Should the Commission Be Both Prosecutor and Judge?*, YOUTUBE (Mar. 11, 2014), http://youtu.be/a9zvyDr4a-Y, at 9:24.

> sion to prosecute more transparent. One person would be responsible for the agency's enforcement agenda.[222]

Calvani notes that this would not significantly alter the responsibility of the powers of Commissioners, since "the power of a commissioner is relatively slight. The only real power of a commissioner is a negative one: blocking an enforcement initiative."[223] But it would "rather dramatically, [the responsibilities] of the chair."[224] In our view, this is a bug, not a feature.

RECOMMENDATION: Abolish or Limit Part III to Settlements

More fundamentally, Congress should re-examine the continued need for Part III as an alternative to litigation in Federal court. There are important differences between adjudications that originate in Part III proceedings as opposed to those that originate in Article III proceedings. Foremost, the selection of venue is an important determinant of the FTC's likelihood of success as well as the level of deference it will enjoy. Defendants will likewise see major differences between litigation in the different fora: from the range of discovery options available to the range and sort of materials considered by the tribunal (e.g., through amicus briefs). And, perhaps most important, the different venues each will create different legal norms and rules binding upon parties to future proceedings.

There is also a question regarding to what extent Part III proceedings are more than a mere formality. On the one hand, the FTC's Administrative Law Judge takes his job seriously, and has reversed the Commission in, most notably, two recent consumer protection decisions.[225] However, on the other hand, the Commission *always* reverses decisions of the ALJ that find against it.[226] Which leads to an important question: if the Commission is simply going to reverse its ALJ anyway what is the point of having an ALJ?

Even the threat of Part III litigation has a significant effect in coercing defendants to settle with the FTC during the investigation stage — not merely because of the direct financial costs of two additional rounds of litigation (first before the ALJ and then before the full Commission) prior to facing an independent Article III tribunal, but also because the Part III process drags out the other, less tangible but potentially far greater costs to the company in reputation and lost management attention. The threat of suffering two rounds of bad

---

[222] Calvani & Diveley, *supra* note 219, at 1184.

[223] *Id.* at 1185.

[224] *Id.* at 1184.

[225] In the Matter of LabMD, Inc., FTC File No. 102 3099 (May 16, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter; POM Wonderful LLC v. FTC, 777 F.3d 478 (D.C. Cir. 2015).

[226] Joshua D. Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, CPI ANTITRUST CHRONICLE, 4 (2012).

press before going to federal court (or at least one, if the ALJ rules for a defendant but the Commission reverses) may persuade some defendants who wouldn't otherwise to settle. Thus, the current operation of Part III rarely, if ever, serves to actually advance the interests of a fair hearing on disputed issues, and is more a tool to coerce settlements.

Congress could end this dynamic by requiring the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery. This is not a novel idea, nor would it be disruptive to the FTC as the Commission has had independent litigating authority since the 1970s.[227] The Smarter Act (H.R. 2745) effectively abolishes Part III with respect to merger cases, by requiring the FTC to bring Clayton Act Section 7 cases (for preliminary injunctions to stop mergers) in federal court under the same procedures as the Department of Justice.[228] This bill passed by a vote of 230 to 170.[229]

Finally, those who might object that abolishing Part III would hamstring the agency should take comfort in the fact that the FTC uses Part III so rarely anyway. Abolishing Part III will not bury the FTC in an avalanche of litigation in federal court. At most it would marginally increase the willingness of companies to resist the siren song of settlement, thus resulting in slightly more litigation (and perhaps also slightly more cases simply abandoned by staff, if they do not think they could win). But this is a trivial price to pay in comparison with the benefit of getting more judicial review and consistent enforcement standards and judicial standards of review. The difference between essentially no litigation and *some* litigation is the key difference between the Discretionary and Evolutionary Models.

RECOMMENDATION: Allow Commissioners to Limit the Use Part III

The least draconian reform would be to empower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective.

---

[227] Elliott Karr, *Essay: Independent Litigation Authority and Calls for the Views of the Solicitor General*, 77 GEO. WASH. L. REV. 1080, 1090-91 (2009).

[228] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/2745 [hereinafter SMARTER Act].

[229] U.S. House of Rep., *Final Vote Results For Roll Call 137* (Mar. 23, 2016) available at http://clerk.house.gov/evs/2016/roll137.xml

Standard for Settling Cases

No Bill Proposed

RECOMMENDATION: Set a Standard for Settling Cases Higher than for Bringing Complaints

Currently there is no standard for settling cases. The Commission simply applies the "reason to believe" standard set forth in Section 5(b) — and very often combines the vote as to whether to bring the complaint with the vote on whether to settle the matter, when the staff has already negotiated the settlement during the investigation process (because of the enormous leverage it has in this process, as we explain above). As Commissioner Wright has noted, "[w]hile the Act does not set forth a separate standard for accepting a consent decree, I believe that threshold should be at least as high as for bringing the initial complaint."[230] Reform in this area is especially critical if Congress chooses not to enact the "preponderance of the evidence" standard for issuing complaints.[231]

While it would certainly be an improvement to adopt even a "preponderance of the evidence" standard for the approval of consent decrees (relative to the status quo), we believe that this should be the standard for the approval of *complaints*, and that approval of *consent decrees* should be even higher (although, as we emphasis above, the "preponderance of the evidence" is not a particularly high standard).[232] The standard and process required by the Tunney Act for antitrust settlements would be a good place to begin. That act requires the FTC to file antitrust consent decrees with a federal court, and requires the court make the following determination:

> Before entering any consent judgment proposed by the United States under this section, the court shall determine that the entry of such judgment is in the public interest. For the purpose of such determination, the court shall consider:
>
> (A) the competitive impact of such judgment, including termination of alleged violations, provisions for enforcement and modification, duration of relief sought, anticipated effects of alternative remedies actually considered, whether its terms are ambiguous, and any other competitive considerations bearing upon the adequacy of such judgment that the court deems necessary to a determination of whether the consent judgment is in the public interest; and

---

[230] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Nomi Technologies, Inc., FTC. File No. 132 3251 (Sept. 3, 2015), 2, *available at* https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

[231] See, *supra*, at 18.

[232] *See infra* at 18.

> (B) the impact of entry of such judgment upon competition in the relevant market or markets, upon the public generally and individuals alleging specific injury from the violations set forth in the complaint including consideration of the public benefit, if any, to be derived from a determination of the issues at trial.[233]

If anything, a standard for settlements should require *more* analysis than this, as the Tunney Act has been relatively ineffective. In particular, any approach based on the Tunney act should allow third parties to intervene to challenge the FTC's assertions about the public interest.[234] This reform could go a long way toward inspiring the agency to perform more rigorous analysis.

Competition Advocacy

The FTC occupies a unique position in its role as the federal government's competition scold. Despite the absence of direct legal authority over federal, state and local actors (which limits the efficacy of competition advocacy efforts), some have argued that "the commitment of significant Commission resources to advocacy is nonetheless warranted by the past contributions of competition authorities to the reevaluation of regulatory barriers to rivalry, and by the magnitude and durability of anticompetitive effects caused by public restraints on competition."[235]

The FTC performs two different, but related, kinds of "competition advocacy":

1. **Competition advocacy *litigation***: The Bureau of Competition occasionally brings antitrust cases against nominally public bodies that the FTC believes are ineligible for state action immunity, either because they are effectively operating as marketplace participants (*e.g.*, state-run hospitals) or because state-created regulatory boards have been so completely coopted by private actors that they operate as private cartels, lacking sufficiently clear statement of legislative intent to maintain their state action immunity.
2. **Competition advocacy *filings***: The Office of Policy Planning files comments with state, local, tribal and federal lawmakers and regulators as to the impact of proposed (or existing) legislation or regulation upon consumers and competition.

---

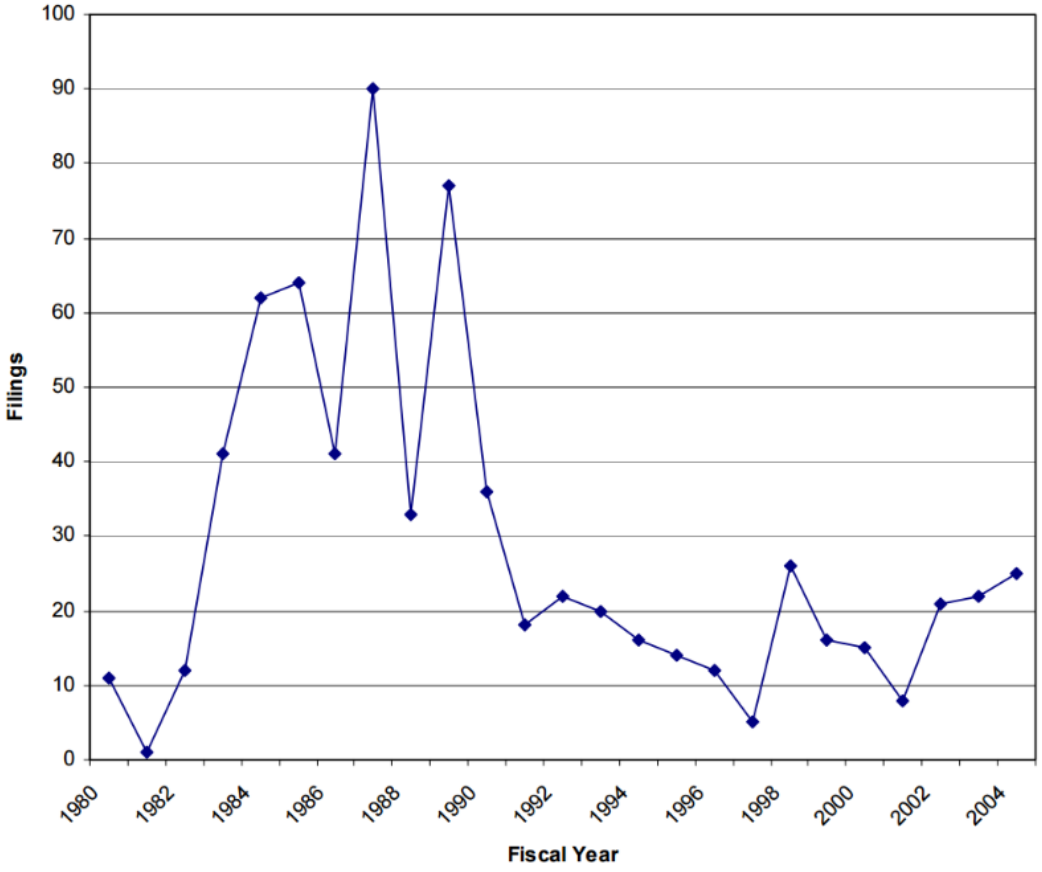
[233] 15 U.S.C. § 16(b)(1).

[234] The act currently provides that "Nothing in this section shall be construed to require the court to conduct an evidentiary hearing or to require the court to permit anyone to intervene." 15 U.S.C. § 16(b)(2).

[235] Ernest Gellhorn, & William E. Kovacic, *Analytical Approaches and Institutional Processes for Implementing Competition Policy Reforms by the Federal Trade Commission* (Dec. 12, 1995), *available at* https://www.ftc.gov/system/files/documents/public_statements/418071/951212comppolicy.pdf.

In 2004, James Cooper, Paul Pautler and Todd Zywicki (all FTC veterans) provided an empirical basis for comparing the FTC's level of activity on competition advocacy filings.[236] Their analysis included this chart:

FTC Advocacy Filings, 1980 to 2004[237]



Since 2009, the FTC has averaged just nineteen competition advocacy filings per year.[238] On high-tech matters, the Commission has been particularly inactive, making just four filings on ride-sharing,[239] four on direct sale of cars to consumers (*i.e.*, online),[240] and none on

---

[236] James C. Cooper, Paul A. Pautler & Todd J. Zywicki, *Theory and Practice of Competition Advocacy at the FTC* at 3, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/FTC%2090th%20Anniversary%20Symposium/040910zywicki.pdf.

[237] *Id.*

[238] A search of the FTC's Advocacy Filings reveals that between January 2009 and January 2016, 115 separate documents have been filed. *See* Fed Trade Comm'n, Advocacy Filings *available at* https://www.ftc.gov/policy/advocacy/advocacy-filings.

[239] Fed Trade Comm'n, "Transportation" Advocacy Filings, *available at* https://www.ftc.gov/policy/advocacy/advocacy-filngs?combine=&field_matter_number_value=&field_advocacy_document_terms_

(cont.)

house-sharing. It has also made few other broadly tech-related miscellaneous filings to other federal agencies on privacy and data security, vehicle-to-vehicle communications, mobile financial services, and the National Broadband Plan.

The FTC held a workshop on the sharing economy in June 2015,[241] but has since missed the opportunity to do significant competition advocacy work in the area, despite growing protectionist state and local regulation aimed at upstarts like Uber, Lyft, Airbnb and others. Recent legislation in Austin, Texas, is sadly illustrative. An Austin City Council ordinance,[242] essentially regulating ride-sharing services out of existence, was approved by (the few) voters who showed up to vote in a referendum.[243] This type of overly broad law regulating innovative technology is exactly the sort of thing the FTC should be taking initiative to advocate against, and it is unfortunate that, in the face of it, the FTC's competition advocacy has receded.

By contrast, in the early 2000s, OPP's State Action Task Force and Internet Task Force made a concerted effort to challenge anticompetitive state and local regulations that hindered online commerce through litigation, testimony and comments. The FTC started several campaigns, including one challenging rules making it harder to participate in e-commerce. Unlike the current Commission's stunted approach, the early 2000s FTC started with a workshop,[244] released reports explaining the problem the FTC's planned approach,[245]

---

tid=5283&field_date_value%5Bmin%5D%5Bdate%5D=January%2C+2009&field_date_value%5Bmax%5D%5Bdate%5D=January%2C+2016&items_per_page=100.

[240] Fed Trade Comm'n, "Automobiles" Advocacy Filings, *available at* https://goo.gl/lq9ACP.

[241] Fed. Trade Comm'n, The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators (Jun. 9, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators

[242] Austin, Texas, Ordinance No. 20151217-075 (2015), *available at* http://www.austintexas.gov/edims/document.cfm%3Fid=245769.

[243] Jared Meyer, *The Reverse of Progress. Austin's new rules strangle Uber, Lyft – and the ridesharing economy,* U.S. NEWS & WORLD REPORT (May 18, 2016), *available at* http://www.usnews.com/opinion/articles/2016-05-18/austins-very-un-progressive-example-on-uber-and-lyft.

[244] Fed. Trade Comm'n Workshop, Possible Anticompetitive Efforts to Restrict Competition on the Internet, Oct. 8-10, 2002, *available at* https://www.ftc.gov/news-events/events-calendar/2002/10/possible-anticompetitive-efforts-restrict-competition-internet.

[245] FED. TRADE COMM'N, REPORT OF THE STATE ACTION TASK FORCE (2003), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/report-state-action-task-force/stateactionreport.pdf; FED. TRADE COMM'N, POSSIBLE ANTICOMPETITIVE BARRIERS TO E-COMMERCE: WINE (2003), *available* at https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-report-concerning-possible-anticompetitive-barriers-e-commerce-wine/winereport2.pdf; FED. TRADE COMM'N, POSSIBLE BARRIERS TO E-COMMERCE: CONTACT LENSES: A REPORT FROM THE STAFF OF THE FEDERAL TRADE COMMISSION (Mar. 29, 2004), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/possible-anticompetitive-barriers-e-commerce-contact-lenses-report-staff-ftc/040329clreportfinal.pdf.

and then went on to systematically challenge e-commerce-related regulations (among other things) inconsistent with consumer welfare. Filings included:

- Comment on Ohio legislation to allow direct shipment of wine to Ohio consumers;[246] and on similar New York legislation;[247]
- Congressional Testimony regarding online wine sales;[248]
- Comment on Arkansas legislation regarding online contact sales;[249] and
- Comment on Connecticut regulation of contact sales.[250]

The current FTC has many ripe targets for public interest advocacy around the nation as incumbents are, predictably, using regulation to try to stop Internet- and app-based competition, especially disruptive new "sharing economy" business models.

VALUE OF THE IDEA: Competition Advocacy Is the Most Cost-Effective Way to Serve Consumers

As Cooper, Pautler & Zywicki explain:

> The economic theory of regulation ("ETR") posits that because of relatively high organizational and transaction costs, consumers will be disadvantaged relative to businesses in securing favorable regulation. This situation tends to result in regulations — such as unauthorized practice of law rules or per se prohibitions on sales-below-cost — that protect certain industries from competition at the expense of consumers. Competition advocacy helps solve consumers' collective ac-

---

[246] Comment on Proposed Direct Shipment Legislation of the Federal Trade Commission to the Ohio State Senate (2006), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-eric-d.fingerhut-concerning-ohio-s.b.179-allow-direct-shipment-wine-ohio-consumers/v060010commentreohiosb179directshipmentofwine.pdf

[247] *Letter of the Federal Trade Commission regarding Assembly bill 9560-A, Senate bills 6060-A and 1192 to the New York State legislature (2004)*, https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-william-magee-et-al.concerning-new-york.b.9560-s.b.606-and-s.b.1192-allow-out-state-vendors-ship-wine-directly-new-york-consumers/v040012.pdf

[248] Prepared Statement of Todd Zywicki, Fed. Trade Comm'n, before the Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce United States House of Representatives (Oct. 13, 2003), available at https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-statement-u.s.house-representatives-energy-and-commerce-concerning-e-commerce-wine-sales-and-direct-shipment/031030ecommercewine.pdf

[249] *Letter of the Federal Trade Commission regarding Arkansas HB 2286 to the Arkansas House of Representatives (2015)*, *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-doug-matayo-concerning-arkansas-h.b.2286-and-fairness-contact-lens-consumers-act-and-contact-lens-rule/041008matayocomment.pdf.

[250] Comments of the Staff Of the Federal Trade Commission In Re: Declaratory Ruling Proceeding on the Interpretation and Applicability of Various Statutes and Regulations Concerning the Sale of Contact Lenses (2002), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-connecticut-board-examiners-opticians-intervenor-re-declaratory-ruling-proceeding/v020007.pdf

> tion problem by acting within the political system to advocate for regulations that do not restrict competition unless there is a compelling consumer protection rationale for imposing such costs on citizens. Furthermore, advocacy can be the most efficient means to pursue the FTC's mission, and when antitrust immunities are likely to render the FTC impotent to wage ex post challenges to anticompetitive conduct, advocacy may be the only tool to carry out the FTC's mission.[251]

Competition advocacy is probably the most cost-effective way the FTC can promote consumer welfare. Anticompetitive practices and agreements backed up by the power of the state are much less likely to be corrected by the power of competition than those that exist in the marketplace, and antitrust law cannot be used to remove such barriers to competition. The only way for the FTC to even get at such conduct is through its competition advocacy arm.

RECOMMENDATION: Clarify Section 6(f) & the FTC May File Unsolicited Comments

The FTC currently relies on Sections 6(a) (information gathering) and 6(f) (issuance of reports) as the basis for its competition advocacy filings.[252] But as discussed above,[253] Section 6(f) could be read to allow the FTC to make recommendations for legislation only to Congress, not to states or local governments. This is the kind of small discontinuity between the statute's plain meaning and the agency's practice (on an issue that enjoys broad bipartisan support) that should be addressed by Congress in regular reauthorization.

In the same vein, we gather that, if only by standing convention, the FTC does not file comments with state and local lawmakers or regulators unless invited to do so by someone on the relevant body. This is undoubtedly well-intentioned, perhaps grounded in some kind of sense of federalism, but it may have the perverse result of denying consumers the benefit of the FTC's competition-advocacy work where it is most needed: when state regulators are so captured by incumbents, or otherwise blinded to the benefits of new technologies, that they will resent the FTC's comment as an intrusion upon their decision-making.

We urge Congress to kill two birds with one stone by amending Section 6(f) to add the following bolded text (and, for clarity's sake, roman numeral subsection numbers):

---

[251] Cooper, Pautler & Zywicki, *Theory and Practice of Competition Advocacy at the FTC supra* note 236, at 2.

[252] See, e.g., *id.* at 1, n.3:

> The legal authority for competition advocacy is found in Section 6 of the FTC Act, which allows the FTC to "gather and compile information" that concerns persons subject to the FTC Act, and "to make public such portions of the information obtained" that are "in the public interest."

(Quoting 15 U.S.C. § 46(a), (f) (2005)).

[253] *See supra* 61.

> To (i) make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to (ii) make annual and special reports to the Congress and to submit therewith recommendations for additional legislation; ***and to (iii) file recommendations for legislation or regulatory action with state, local, tribal and federal bodies***; and to (iv) provide for the publication of its reports and decisions in such form and manner as may be best adapted for public information and use

RECOMMENDATION: Create an Office of Bureau of Competition Advocacy with Dedicated Funding

The FTC's Competition advocacy *filing* function has languished, in part, because while competition advocacy *litigation* resides inside the Bureau of Competition, the filings are primarily the responsibility of the Office of Policy Planning (OPP), a relatively tiny organization attached to the Chairman's office, which has a staff of just over a dozen compared to 285 for the Bureau of Competition, 331 for the Bureau of Consumer Protection, and 114 for the Bureau of Economics.[254]

Congress should seriously consider creating an independent office of Competition Advocacy, which would manage competition-advocacy filings, and share joint responsibility for competition-advocacy litigation with the Bureau of Competition. In particular, this would mean giving this new Bureau a line item in the FTC's budget.

RECOMMENDATION: In the Alternative, Reconstitute the Task Force

As noted above, the Internet Task Force, which was spun off from the broader State Action Task Force, had considerable effect through its research, reports, and associated filings. A standing Task Force of this nature could provide dividends by picking up where the Sharing Economy Workshop left off and studying the effects of regulation on the sharing economy around the nation. A well-done report could then be followed by strategic litigation, amicus briefs, and other filings in order to promote sound public policy and combat the Internet-age protectionism that is slowing down innovation and competition and the attendant benefit to consumers.

Expanding FTC Jurisdiction

Section 5 of the FTC Act empowers the Commission to prevent unfair and deceptive acts and practices by nearly all American businesses (and business people). The exceptions are

---

[254] *Cf.* Fed. Trade Comm'n, Federal Trade Commission Office of Policy Planning Organizational Chart, https://www.ftc.gov/system/files/attachments/office-policy-planning/opp-org-chart-may2016.pdf; Fed. Trade Comm'n, Shutdown of Federal Trade Commission Operations Upon Failure of the Congress to Enact Appropriations, https://www.ftc.gov/system/files/attachments/office-executive-director/130925ftcshutdownplan.pdf.

few: "banks, savings and loan institutions…, federal credit unions…, common carriers subject to the Acts to regulate commerce, air carriers and [certain meat packers and stockyards]...." One important limitation is that the FTC Act does not expressly give the Commission jurisdiction over nonprofit organizations. Nevertheless, courts have held that nonprofit status is not in itself sufficient to exempt an organization from FTC jurisdiction.[255] In *Cal Dental Ass'n v. FTC*, the Supreme Court noted that the FTC has jurisdiction over both "'an entity organized to carry on business for its own profit' … [as well as] one that carries on business for the profit 'of its members.'"[256] Thus, various types of nonprofits — notably trade associations — can be reached by the FTC *depending on their activities*, but "purely charitable" organizations remain outside of the FTC's enforcement purview.[257]

Subcommittee Democrats have revived two sensible proposals from 2008 to expand the FTC's jurisdiction. Both have long enjoyed bipartisan support, and have been endorsed by the Commission under both Republican and Democratic chairmen.

FTC Jurisdiction over Common Carriers

The Protecting Consumers in Commerce Act of 2016

Jerry McNerney's (D-CA) bill (H.R. 5239)[258] would allow the FTC to regulate common carriers currently regulated by the Federal Communications Commission. In particular, this would ensure that the FTC and FCC have dual jurisdiction over broadband — effectively restoring the jurisdiction the FTC lost when the FCC "reclassified" broadband in 2015.

The FCC recently issued a controversial NPRM proposing privacy and data security rules for broadband that are significantly different from the approach the FTC has taken. This bill would moot the need for new FCC privacy and data security rules as a "gap filler." The bill would also allow the FTC to police net neutrality concerns, interconnection and other broadband practices (to the extent it finds unfair or deceptive practices) even if the FCC's Open Internet Order fails in pending litigation.

---

[255] *See, e.g.*, Community Blood Bank v. FTC, 405 F.2d 1011 (8th Cir. 1969).

[256] Cal. Dental Ass'n v. FTC, 526 U.S. 756, 766 (1999).

[257] *See Statement of William C. Macleod, Dir. of FTC Bureau of Consumer Protection, Before The U.S. House of Representatives Committee on Energy & Commerce; Subcommittee on Transportation & Hazardous Materials; Hearing On Deceptive Fundraising By Charities* (Jul. 28, 1989), *available at* http://www.freespeechcoalition.org/macleod.htm.

[258] Protecting Consumers in Commerce Act of 2016, H.R. 5239, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/5239/text.

VALUE OF THE BILL: Reclassification of Broadband by the FCC Should Not Remove FTC Jurisdiction

There has long been unusual bipartisan agreement on ending the common carrier exemption. This was proposed by Sen. Byron Dorgan's proposed FTC Reauthorization Act of 2002,[259] and supported by Republican Commissioner Thomas Leary and Democrat Commissioner Sheila Anthony.[260] Sen. Dorgan last proposed the same reform in 2008.[261] More recently, in 2015, Democrat Chairman Edith Ramirez and Republican Commissioner Josh Wright supported this reform.[262]

Section 5 jurisdiction excludes "common carriers subject to the Acts to regulate commerce."[263] The bill simply edits the definition of "Acts to regulate commerce" in Section 4 to remove the Communications Act.[264] Thus, the FTC *could* regulate common carriers regulated by the FCC but *not* transportation common carriers.

Former Commissioner Joshua Wright summarized the many advantages of keeping the FTC as a cop on the broadband beat:

> The FTC has certain enforcement tools at its disposal that are not available to the FCC. Unlike the FCC, the FTC can bring enforcement cases in federal district court and can obtain equitable remedies such as consumer redress. The FCC has only administrative proceedings at its disposal, and rather than obtain court-ordered consumer redress, the FCC can require only a "forfeiture" payment. In addition, the FTC is not bound by a one-year statute of limitations as is the FCC. The FTC's ability to proceed in federal district court to obtain equitable remedies that fully redress consumers for the entirety of their injuries provides comprehen-

---

[259] Federal Trade Commission Reauthorization Act of 2002, S. 2946, 104th Cong. (2002), *available at* https://www.congress.gov/bill/107th-congress/senate-bill/2946/text.

[260] *Additional Statement of Commissioner Thomas B. Leary*, *Hearing Before the H. Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2003), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-reauthorization/030611learyhr.pdf; Federal Trade Commission Testifies Before Senate in Support of Reauthorization Request for Fiscal Years 2003 to 2005, *available at* https://www.ftc.gov/es/node/63553.

[261] Federal Trade Commission Reauthorization Act of 2008, S. 2831 §14, 110th Cong. (2008), *available at* https://www.govtrack.us/congress/bills/110/s2831/text

[262] *Prepared Statement of Commissioner Joshua D. Wright, Federal Trade Commission: Wrecking the Internet to Save It? The FCC's Net Neutrality Rule Before the H. Comm. on the Judiciary*. 114th Cong. (2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/632771/150325wreckinginternet.pdf; Ramirez urges repeal of common carrier exemption, FTC WATCH, *available at* http://www.ftcwatch.com/ramirez-urges-repeal-of-common-carrier-exemption/.

[263] 15 U.S.C. § 45(a)(2).

[264] *Cf.* 15 U.S.C. § 44.

sive consumer protection and can play an important role in deterring consumer protection violations.[265]

RECOMMENDATION: Pass the Protecting Consumers in Commerce Act to End the Exemption for Telecom Common Carriers

Ending the common carrier exemption for telecom companies is long overdue. "As the telecommunications and Internet industries continue to converge, the common carrier exemption is likely to frustrate the FTC's efforts to combat unfair or deceptive acts and practices and unfair methods of competition in these interconnected markets."[266] Moreover, the uncertainty surrounding the application of the exemption to new technologies, as well as the long-standing uncertainty around application of the exemption to non-common-carrier activities carried out by common carriers introduce needless administrative costs.

RECOMMENDATION: Require the FCC to Terminate Its Privacy Rulemaking

With respect to the common carrier exception, the fortunes of the FTC are tied to those of the FCC; adopting optimal policy for one requires adopting complimentary policy for the other. The conclusions above are complicated by the FCC's ongoing efforts to exercise the *exclusive* authority it claimed when it reclassified Internet service providers as common carriers, particularly with respect to privacy and similar matters.[267] Because the FCC's rationale for its proposed privacy rules is to fill the gap it created by "reclassifying" broadband and thus removing it from the FTC's jurisdiction, enactment of this legislation would moot the need for new FCC rules. Accordingly, this bill should include a provision directing the FCC to terminate that rulemaking — so that the FTC may resume its former role in policing broadband privacy and data security without unnecessary and costly duplicative regulations.

This situation is very much unlike that in the 1980 FTC Improvements Act, by which Congress both tightened the FTC's Section 5 rulemaking processes (as instituted in 1975) and also ended the FTC's children's advertising rulemaking.[268] In signing the bill, President Carter lauded the former but objected to the latter:

---

[265] *Prepared Statement of Commissioner Joshua D. Wright*, *supra, available at* https://www.ftc.gov/system/files/documents/public_statements/632771/150325wreckinginternet.pdf (internal citations omitted).

[266] FED TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION REPORT, 41 (2007), *available at* https://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf.

[267] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, WC Docket No. 16-106 (rel. Apr. 1, 2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

[268] FTC Improvements Act Section 11 added the following language to 17 U.S.C. § 57a: "The Commission shall not have any authority to promulgate any rule in the children's advertising proceeding pending on the date of the enactment of the Federal Trade Commission Improvements Ante, p. 374. Act of 1980 or in any

(cont.)

> We need vigorous congressional oversight of regulatory agencies. But the reauthorization bills passed by the Senate and the House went beyond such oversight and actually required termination of specific, major, ongoing proceedings before the Commission. I am pleased that the conferees have modified these provisions. If powerful interests can turn to the political arena as an alternative to the legal process, our system of justice will not function in a fair and orderly fashion.[269]

President Carter had a point, in general. But in this case, Congress would not be telling an agency to stop a pending rulemaking because of a policy difference; it would be telling the FCC to stop a rulemaking that it claims is necessary only because of a regulatory vacuum of its own creation.

If the FCC insists on issuing its own rules, the bill will result in overlapping jurisdiction, which could create problems of its own: forum-shopping, inconsistent results, and politicization of the enforcement process. The Memorandum of Understanding reached between the two agencies on how to handle enforcement where their authority *does* overlap will do little to minimize potential conflicts.[270] It would be particularly incongruous to enact legislation authorizing overlapping and conflicting jurisdiction while Congress is also considering the SMARTER Act, aimed at mitigating exactly such problematic overlap in the antitrust enforcement authority of the FTC and DOJ.[271] None of these concerns are inherent reasons not to restore the FTC's jurisdiction; after all, the FTC is the better regulator, in large part because applying standards of general applicability makes the FTC a more difficult agency to capture than a sector-specific regulator like the FCC. But these concerns do make it important that passage of this bill be tied to ending the FCC's foray into privacy and data-security regulation.

FTC Jurisdiction over Tax-Exempt Organizations & Nonprofits

The Tax Exempt Organizations Act

Representative Rush's (D-IL) bill (H.R. 5255)[272] would add tax-exempt, 501(c)(3) nonprofits to the definition of "corporation" subject to the FTC Act in Section 4 (15 U.S.C. § 44). It

---

substantially similar proceeding on the basis of a determination by the Commission that such advertising constitutes an unfair act or practice in or affecting commerce."

[269] Carter, *supra* note 19.

[270] Memorandum of Understanding on Consumer Protection Between the Federal Trade Commission and the Federal Communications Commission (Nov. 2015), *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

[271] SMARTER Act, *supra* note 228.

[272] A Bill to Amend the Federal Trade Commission Act to Permit the Federal Trade Commission to Enforce Such Act Against Certain Tax-exempt Organizations, H.R. 5255, 114th Cong. (2016) *available at* https://www.congress.gov/bill/114th-congress/house-bill/5255/text.

would not, however, amend Section 4 to remove the language that limits the FTC's jurisdiction to corporations that "carry on business for [their] own profit or that of [their] members." Thus, the FTC would still be limited to policing for-profit activities but would have an easier time establishing that a nonprofit was essentially conducting for-profit activities.

VALUE OF THE BILL: Would Reduce Litigation Expenses for the FTC

This bill does precisely the same thing proposed by Sen. Byron Dorgan's FTC Reauthorization Act of 2008.[273] The Republican-led FTC supported this provision at the time.[274]

In 2008, in supporting Sen. Dorgan's version of this bill, the FTC explained the advantage of this reform, even though it would not technically change the substance of the FTC's jurisdiction:

> The proposed legislation would also help increase certainty and reduce litigation costs in this area. Although the FTC has been successful in asserting jurisdiction against "sham" nonprofits and against non-profit trade associations, the proposed legislation would help avoid protracted factual inquiries and litigation battles to establish jurisdiction over such entities.[275]

We agree with the FTC's 2008 assessment.

RECOMMENDATION: Extend Jurisdiction to Tax-Exempt Entities, Including Trade Associations

In 2008, in supporting Sen. Dorgan's version of this bill, the FTC also said:

> The Commission would be pleased to work with Congressional staff on crafting appropriate language. The Commission notes that, as drafted, Section 6 would reach only those non-profit entities that have tax-exempt status under section 501(c)(3) of the Internal Revenue Code. The Commission would benefit from broadening this provision to cover certain other nonprofits, such as Section 501(c)(6) trade associations. The Commission has previously engaged in protracted litigation battles to determine whether such entities are currently covered under the FTC Act. *See, e.g., California Dental Ass'n v. FTC*, 526 U.S. 756, 765-69 (1999) (holding that FTC Act applies to anticompetitive conduct by non-profit dental association whose activities provide substantial economic benefits to for-profit members); *American Medical Ass'n v. FTC*, 638 F.2d 443, 447-448 (1980) (finding FTC jurisdiction over non-profit medical societies whose activities

---

[273] Federal Trade Commission Reauthorization Act of 2008, *supra* note *261*, § 6, *available at* https://www.govtrack.us/congress/bills/110/s2831/text.

[274] *Prepared Statement of the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Science, and Transportation*. 110th Cong. (2008), 19, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/ftc-testimony-reauthorization/p034101reauth.pdf.

[275] *Id*. at 16.

"serve both the business and non-business interests of their member physicians").[276]

RECOMMENDATION: Extend Jurisdiction to *All* Non-Profits

We likewise recommend expanding the bill to encompass all nonprofit corporations, regardless of their tax-exempt status.[277] The logic of the FTC's jurisdiction doesn't turn on the tax-exempt status of organizations, which, for these purposes, is essentially a meaningless dividing line between entities. It makes little sense to include tax-exempt nonprofits within the FTC's ambit while excluding nonprofits without federal tax-exempt status.

Rulemaking

The FTC makes rules in two ways: (1) under Section 5, through the process created by Congress in 1980 to require additional economic rigor and evidence; and (2) under narrow grants of standard APA rulemaking authority specific to a particular issue.

Economic Analysis in All FTC Rulemakings

No Bill Proposed

RECOMMENDATION: Require BE to Comment on Rulemakings

The RECS Act, discussed below, would require the FTC to include BE analysis of any recommendations it makes for rulemakings. However, this would not apply to the FTC's own rulemakings because that bill is focused on the FTC's statutory authority to make recommendations to Congress, other agencies, and state and local governments.

Requiring regulatory agencies to do cost-benefit analysis has been uncontroversial for decades, dating back at least to the Carter Administration. Indeed, in 2011, shortly after President Obama issued Executive Order 13563,[278] his version of President Clinton's 1993 Executive Order 12866[279] applying to Executive Branch agencies, he issued a second order, Regu-

---

[276] *Id.* at 18 n.49.

[277] The nonprofit designation is a creature of state incorporation law, and obligates corporations to adopt certain governance rules and structures. Federal tax-exempt status is a creature of federal tax law, and, while it obligates companies to limit their corporate purpose (*e.g.*, to education, religious activities, etc.), it doesn't appreciably affect their governance structure. Companies can be nonprofit but not tax-exempt, although all tax-exempt companies are nonprofit.

[278] Exec. Order No. 13,563, 3 C.F.R. 13563 (2012) *available at* https://www.whitehouse.gov/the-press-office/2011/01/18/executive-order-13563-improving-regulation-and-regulatory-review.

[279] Exec. Order No. 12,866 3 C.F.R. 12866 (1993) *available at* https://www.whitehouse.gov/sites/default/files/omb/inforeg/eo12866/eo12866_10041993.pdf.

lation and Independent Regulatory Agencies, Executive Order 13579.[280] The key difference between the two is that the President said Executive agencies "must" do cost-benefit analysis for each new regulation, but that independent agencies "should" undertake retrospective analysis of its rules and periodically update them.

FTC Chairman Jon Leibowitz fully endorsed the idea in the White House's blog about the Order:

> President Obama deserves enormous credit for ensuring regulatory review throughout the federal government, including at independent agencies. Although regulations are critically important for protecting consumers, they need to be reviewed on a regular basis to ensure that they are up-to-date, effective, and not overly burdensome. For all agencies – independent or not – periodic reviews of your rules is just good government. The announcement raises the profile of this issue, and I think that's a constructive step.[281]

The chief (indeed, perhaps the only) reason for the difference is that the President has no authority over independent agencies, which are creatures and servants of Congress. The bipartisan Independent Agency Regulatory Analysis Act of 2015 (S. 1607) would solve this problem, giving the President the authority to set cost-benefit standards for independent agencies as well.[282] We fully support that bill and believe this requirement should apply to *all* independent agencies. But there is no reason to wait for passage of the more comprehensive bill. The FTC in particular would benefit from a commitment to cost-benefit analysis in its rulemakings immediately.

Of course, it is true that the Commission has abandoned using its Section 5 rulemaking power (precisely because it reflects the Carter-era commitment to cost-benefit analysis). But the Commission *does* continue to make rules under a variety of issue-specific statutes such as several of those now pending before the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade in May 2016.[283] As the chief example of the need for greater economic rigor in FTC rulemakings, we note the FTC's 2012 COPPA rulemaking: the agency expanded the definition of "personal information," thus greatly

---

[280] Exec. Order No. 13,579, 3 C.F.R. 13579 (2012) *available at* https://www.whitehouse.gov/the-press-office/2011/07/11/executive-order-13579-regulation-and-independent-regulatory-agencies.

[281] Cass Sunstein, *The President's Executive Order on Improving and Streamlining Regulation by Independent Regulatory Agencies*, WHITEHOUSE.GOV BLOG (Jul. 11, 2011), https://www.whitehouse.gov/blog/2011/07/11/president-s-executive-order-improving-and-streamlining-regulation-independent-regula.

[282] Independent Agency Regulatory Analysis Act of 2015, S. 1607, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/1607/text.

[283] *See* Press Release, HEARING: #SubCMT to Review 17 Bills Modernizing the FTC for the 21st Century NEXT WEEK, THE ENERGY AND COMMERCE COMMITTEE (May 17, 2016), https://energycommerce.house.gov/news-center/press-releases/hearing-subcmt-review-17-bills-modernizing-ftc-21st-century-next-week.

expanding the number of children's-oriented media subject to the rule, with no meaningful analysis of what this would do to children's media.

Despite loud protests from small operators that the rule might cause them to cease offering child-oriented products, the FTC produced a meaningless estimate that the rule would cost $21.5 million in the aggregate.[284] Of course, the *real* cost of the new rule is not the direct compliance cost but the second-order effects of the number of providers who exit the children's' market, reduce functionality, slow innovation or raise prices — none of which did the FTC even attempt to estimate. This was a clear failure of economic analysis.

We also note Commissioner Ohlhausen's 2015 dissent from the Commission's vote to update the Telemarketing Sales Rule to ban telemarketers from using four "novel" payment methods. Ohlhausen cited no less an authority than the Federal Reserve Bank of Atlanta (FRBA), which is not merely one of twelve Federal Reserve Branches, but the one responsible for "operat[ing] the Federal Reserve System's Retail Payments Product Office, which manages and oversees the check and Automated Clearing House (ACH) services that the Federal Reserve banks provide to U.S. financial institutions."[285] Ohlhausen explained:

> The amendments do not satisfy the third prong of the unfairness analysis in Section 5(n) of the FTC Act, which requires us to balance consumer injury against countervailing benefits to consumers or competition. Although the record shows there is consumer injury from the use of novel payment methods in telemarketing fraud, it is not clear that this injury likely outweighs the countervailing benefits to consumers and competition of permitting novel payments methods….
>
> In sum, the FRBA's analysis of the prohibition of novel payments in telemarketing indicates that any reduction in consumer harm from telemarketing fraud is outweighed by the likely benefits to consumers and competition of avoiding a fragmented law of payments, not limiting the use of novel payments prematurely, and allowing financial regulators working with industry to develop better consumer protections.[286]

Again, it appears that the Commission majority failed to undertake an economically rigorous analysis of the sort BE would likely perform, in this case failing to properly weigh injury and countervailing benefits as Section 5(n) requires.

---

[284] 78 Fed. Reg. 4002 *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

[285] Separate Statement of Commissioner Maureen K. Ohlhausen, Dissenting in Part, In the Matter of the Telemarketing Sales Rule, Project No. R411001, at n. 3 (Nov. 18, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/881203/151118tsrmkospeech.pdf.

[286] *Id.* at 1-2.

At a minimum, the Commission would have done well to solicit further public comment on its rule, heeding the experience of past chairmen, as summarized by Former Chairman Tim Muris:

> By their nature, however, rules also must apply to legitimate actors, who actually deliver the goods and services they promise. Remedies and approaches that are entirely appropriate for bad actors can be extremely burdensome when applied to legitimate businesses, and there is usually no easy or straightforward way to limit a rule to fraud. Rather than enhancing consumer welfare, overly burdensome rules can harm the very market processes that serve consumers' interests. For example, the Commission's initial proposal for the Telemarketing Sales Rule was extremely broad and burdensome, and one of the first acts of the Pitofsky Commission was to narrow the rule. More recently, the Commission found it necessary to re-propose its Business Opportunity Rule, because the initial proposal would have adversely affected millions of self-employed workers.[287]

Issue-Specific Rulemakings

Several Bills Proposed

Congress has long enacted legislation tasking the FTC with enacting regulations in a specific area through standard rulemaking under the Administrative Procedure Act. This, in effect, has allowed the FTC to avoid having to conduct rulemakings under the Magnuson-Moss Act of 1975 (as amended in 1980). The result has been that there may not be anyone left at the FTC who has ever conducted a Section 5 rulemaking. This contributes to the common misconception that the FTC lacks rulemaking authority — something the Chairman and other Commissioners have said casually. Of course, they mean that the FTC lacks *APA* rulemaking authority, and that they believe Section 5 rulemaking is too difficult.

But this belief is unfounded. There is good reason to think that the FTC could have conducted a Section 5 rulemaking to address telemarketing complaints, for example, in about the same amount of time it took Congress to pass the Do Not Call Act and for the FTC to conduct an APA rulemaking, and perhaps even less. As Former Chairman Tim Muris explained, in 2010:

> The Commission's most prominent rulemaking endeavor, the creation of the National Do Not Call Registry, could have proceeded in a timely fashion under Magnuson-Moss procedures. It took two years from the time the rule was first publicly discussed until it was implemented. Although it would have been neces-

[287] *Statement of Timothy J. Muris, supra* note 14, at 24.

> sary to structure the proceedings differently, there would have been little, if any, additional delay from using Magnuson-Moss procedures.[288]

This is not idle speculation. Muris actually ran the FTC during its creation of the Do Not Call registry. Attempting a Section 5 rulemaking would have been a valuable experience for the FTC, and it might have avoided some of the unintended consequences of ex ante legislation.

We make two broad recommendations applicable to all six rulemaking bills.

RECOMMENDATION: Require the FTC to Conduct Section 5 Rulemakings & Report on the Process

The FTC would greatly benefit from conducting a Section 5 rulemaking. Congress should direct the FTC to conduct such a rulemaking on at least one, and preferably two or three, of the issues to be addressed by these proposed issue-specific bills. Having multiple rulemakings would produce a more representative experience with the FTC's Section 5 rulemaking powers. However many Section 5 rulemakings the FTC does, Congress should direct the FTC to report back in, say, three years as to the state of these rulemakings and the FTC's general experience with its Section 5 rulemaking procedures. This is the only way Congress will ever be able to make informed decisions about how existing Section 5 rulemaking processes might be expedited or streamlined without removing the safeguards that Congress rightly imposed to prevent the FTC from abusing its rulemaking powers.

Any reconsideration of the FTC's Section 5 rulemaking processes should be undertaken with the utmost caution. Unfairness is a uniquely elastic concept, which requires unique procedural safeguards if it is to serve as the basis for rulemaking. If anything, FTC's approach to enforcing Section 5 in high tech matters over the last 15–20 years reconfirms the need for safeguards: in its "common law of consent decrees," the FTC has paid little more than lip service to the balancing test inherent in unfairness, and has increasingly nullified the materiality requirement at the heart of the deception policy statement.

RECOMMENDATION: Include Periodic Re-Assessment Requirements in Any New Grants of APA Rulemaking Authority

It is impossible to predict the unintended consequences of any of the proposed issue-specific bills granting the FTC new rulemaking authority.[289] However narrowly targeted they may

---

[288] *Id.* at 27.

[289] *See* Press Release, *#SubCMT Releases Reform Package to Modernize the FTC and Promote Innovation*, THE ENERGY AND COMMERCE COMMITTEE (May 5, 2016), https://energycommerce.house.gov/news-center/press-releases/subcmt-releases-reform-package-modernize-ftc-and-promote-innovation.

seem, they may wind up constraining new technologies or business models that would otherwise serve consumers.

Consider the Video Privacy Protection Act of 1988 ("VPPA"), which barred "wrongful disclosure of video tape rental or sale records."[290] After the experience of Judge Robert Bork, whose video rental records were made an issue at his (failed) Supreme Court confirmation hearings, this quick-fix bill must have seemed utterly uncontroversial. Yet it proved overly rigid in the digital age. In 2009, an anonymous plaintiff sued Netflix over its release of data sets for the Netflix Prize, alleging that the company's release of the information constituted a violation of the VPPA.[291] In 2011 Netflix launched a feature integrating its service with Facebook — everywhere *except* in the U.S., citing the 2009 lawsuit and concerns over the VPPA. After two years, President Obama signed legislation (H.R. 6671) amending the VPPA to allow Netflix and other video companies to *give consumers the option* of sharing information about their viewing history on social networking sites like Facebook.[292] Despite this amendment, the VPPA continues to threaten to overly restrict novel online transactions that were never contemplated or intended by the drafters of the statute.[293]

The VPPA is just one of many laws that have proven unable to keep up with technological change (the 1996 Telecommunications Act, (largely) a classic example of the Rulemaking Model, comes readily to mind). To protect against this inevitability, Congress should include regular review of legislation as a "safety hatch." The 1998 Children's Online Privacy Protection Act (COPPA) included this review provision:

> Not later than 5 years after the effective date of the regulations initially issued under … this title, the Commission shall —
>
> (1) review the implementation of this chapter, including the effect of the implementation of this chapter on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and (2) prepare and submit to Congress a report on the results of the review under paragraph (1).[294]

---

[290] Video Privacy Protection Act of 1988, Pub. L. 100-618, 102 Stat. 3195 (Nov. 5, 1988), *available at* https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf.

[291] *See* Kristian Stout, *Pushing Ad Networks Out of Business: Yershov v. Gannett and the War Against Online Platforms*, TRUTH ON THE MARKET (May 10, 2016), https://truthonthemarket.com/2016/05/10/pushing-ad-networks-out-of-business-yershov-v-gannett-and-the-war-against-online-platforms/.

[292] Video Privacy Protection Act Amendments Act of 2012, H.R. 6671, 112th Cong (2012), *available at* https://www.congress.gov/bill/112th-congress/house-bill/6671?q=%7B%22search%22%3A%5B%22%5C%22hr6671%5C%22%22%5D%7D&resultIndex=1.

[293] *See* Stout, *supra* note 291.

[294] 15 U.S.C. § 6506.

In principle, this is the right idea. However, in practice, this requirement has proven ineffective. The FTC's review of COPPA included little meaningful analysis of the cost of COPPA.[295] Indeed, the FTC used the discretion afforded it by Congress in the statute to expand the definition of the term "personal information" in ways that appear to have reduced the availability, affordability and diversity of children's media — yet without any economic analysis by the Commission.

At a minimum, Congress should include something like the following in any issue-specific grant of new APA rulemaking authority it enacts:

> Not later than 5 years after the effective date of the regulations initially issued under… this title, ***and every 5 years thereafter,*** the Commission shall —
>
> (1) ***direct the Bureau of Economics, with the assistance of the Office of Technology Research and Investigation,*** to review the implementation of this chapter, including the effect of the implementation of this chapter on practices relating to ***[affected industries]***; and
>
> (2) prepare and submit to Congress a report on the results of the review under paragraph (1).

Conclusion

The letter by which the FTC submitted the Unfairness Policy Statement to the Chairman and Ranking Member of the Senate Commerce Committee in December 1980 concludes as follows:

> We hope this letter has given you the information that you require. Please do not hesitate to call if we can be of any further assistance. With best regards,
>
> /s/Michael Pertschuk, Chairman[296]

We believe it's high time Congress picked up the phone.

To be effective, any effort to reform the FTC would require a constructive dialogue with the Commission — not just those currently sitting on the Commission, but past Commissioners and the agency's staff, including veterans of the agency. Along with the community of practitioners who navigate the agency on behalf of companies and civil society alike, all of these will have something to add. We do not presume to fully understand the inner workings of the Commission as only veterans of the agency can. Nor do we presume that the ideas presented here are necessarily the best or only ones to accomplish the task at hand. But reform

---

[295] *See supra* note 284.

[296] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

cannot be effective if it begins from the presumption that today's is the "best of all possible FTCs," or that any significant reform to the agency would cripple it.

Unfortunately, many of those who would tend to know the most about the inner workings of the agency are also the most blinded by status quo bias, the tendency not just to take for granted that the FTC works, and has always worked, well, but to dismiss proposals for change as an attacks upon the agency. It would be ironic, indeed, if an agency that wields its own discretion so freely in the name of flexibility and adaptation were itself unwilling to adapt.

We believe that reforms to push the FTC back towards the Evolutionary Model can be part of a bipartisan overhaul and reauthorization of the agency, just as they were in 1980 and 1994. At stake is much more than how the FTC operates; it is nothing less than the authority of Congress as the body of our democratically elected representatives to steer the FTC. Congress should not, as Justice Scalia warned in 2014 in *UARG v. EPA*, willingly "stand on the dock and wave goodbye as [the FTC] embarks on this multiyear voyage of discovery."[297]

[297] Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2446 (2014).

In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case

Geoffrey A. Manne, R. Ben Sperry & Berin Szoka

ICLE Antitrust & Consumer Protection Research Program
White Paper 2015-1

ICLE | 2325 E Burnside Street, Suite 301 | Portland, OR 97214 | 503.770.0652
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Introduction

Last week the Federal Trade Commission (FTC) settled a privacy case – *In the Matter of Nomi Technologies, Inc.* – that, on its face, will seem banal, but actually raises significant questions about the FTC's understanding of its broad consumer protection authority, especially as applied to cutting-edge technologies. *Nomi* is the latest in a long string of recent cases in which the FTC has pushed back against both legislative and self-imposed constraints on its discretion. By small increments (unadjudicated consent decrees), but consistently and with apparent purpose, the FTC seems to be reverting to the sweeping conception of its power to police deception and unfairness that led the FTC to a titanic clash with Congress back in 1980.

Specifically, the *Nomi* case illustrates that the FTC doesn't think it needs to establish that a misrepresentation was "material" to consumers before finding a statement deceptive under Section 5 of the FTC Act — the very thing that the FTC's 1983 Deception Policy Statement (DPS) was intended to prevent. Effectively nullifying the materiality requirement at the core of the DPS means the FTC is more likely to mis-prioritize its limited enforcement resources, proscribe conduct that actually benefits consumers, and impose remedies that make consumers worse off.

Indeed, that appears to be precisely what will happen here: Out of a desire to encourage — effectively require — companies to disclose data collection, the FTC is actually discouraging companies from doing so (at least in the short run), as Commissioners Ohlhausen and Wright note in their dissents. The FTC majority's blindness to this obvious, but perverse, result suggests that the real purpose of the settlement is strategic: to set a quasi-precedent[1] that the Commission will leverage in the future – probably in harder cases involving more ambiguous conduct – and perhaps also to advance a larger political agenda.

Indeed it is not difficult to guess at what the majority's real agenda is: changing what counts as "reasonable consumer expectations" with regard to tracking and data collection activities generally in order to justify even more aggressive use of Section 5 in the future. Specifically:

1. With this case the FTC is trying to change what it asserts are reasonable consumer expectations about whether consumers are being tracked *without notice* — here, specifically offline, in retail stores, but the same principle could extend to online contexts as well. The majority likely sees *Nomi* as a wedge in this regard, because it believes that it can plausibly (although, as we discuss below, erroneously) make the assertion that "for users who were on notice that tracking might occur, it is reasonable to expect *not* to be tracked without notice."
2. If the FTC enshrines this assertion in enough consent decrees, eventually it will plausibly support a broader assertion that *overall* consumer expectations are that tracking will not occur

---

[1] Settlements are not, of course, binding precedent, *see, e.g.*, Altria Group, Inc. v. Good, 555 U.S. 70, 89 n. 13 (2008) (noting that an FTC "consent order is... only binding on the parties to the agreement"), but they do have a quasi-precedential effect. *See* CONSUMER PROTECTION & COMPETITION REGULATION IN A HIGH-TECH WORLD: DISCUSSING THE FUTURE OF THE FEDERAL TRADE COMMISSION, REPORT 1.0 OF THE FTC: TECHNOLOGY & REFORM PROJECT 24 (Dec. 2013), *available at* http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

without express notification, regardless of whether consumers were specifically put on notice about a *particular* tracking service.

3. Once that asserted transition in consumer expectations occurs, the Commission will be able to bring omission cases against any retailer or any tracking service that engages in data collection (online *or* offline) without conspicuous notice. And once that happens, retailers will also demand that services like Nomi provide notice.
4. In the end, with everyone providing notice all the time, the FTC will eventually bring cases challenging the efficacy of the very opt-out notices it required, and will effectively require *opt-in* to ensure that consumers are not deceived and/or a technological solution that will "push" notifications to consumers' devices in real time (in addition to passive notification like online privacy policies and in-store signage).
5. As a practical matter, the FTC will likely outsource implementation of such a system, which would be difficult to design through the settlement process, to the multistakeholder processes convened by the National Telecommunications and Information Administration (NTIA).

In short, this case is about (i) planting the flag for "proving" that consumer expectations have changed, (ii) getting intermediaries (like retailers) on the hook, (iii) ultimately demanding opt-in for all data-collection and (iv) forcing technological intermediaries like Google and Apple to figure out how to make it all work seamlessly. In effect, the FTC is trying to create, *de facto* and without complicity from Congress, exactly what the Administration's proposed privacy legislation would mandate.[2]

Whatever one thinks about this ultimate outcome, the *process* by which the FTC arrives there should be troubling to everyone. If we are right about what is really going on, that process entails:

- Generously employing the DPS's presumption of materiality to skip ever having to show materiality;
- Subverting the limitations in the DPS by interpreting the presumption of materiality never to require consideration of context, proof of intent or to allow for evidence to rebut the presumption;
- Using case-by-case enforcement (as opposed to industry-wide regulation) to truncate the analysis of key claims to produce "rough cut" ("close enough for government work!") approximations of what the law is; and
- Relying on the propensity of FTC defendants to settle in order to bootstrap those assertions from previous cases into effective "established truths" in subsequent cases without any judicial review.

This would be perhaps the very definition of "abuse of discretion." It would put the "National Nanny" FTC of the 1970s to shame.

---

[2] *See* Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, THE WHITE HOUSE (Feb. 27, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

The Nomi Case

Nomi Technologies offers retailers an innovative technological means to observe how customers move through their stores, how often they return, what products they browse and for how long (among other things) by tracking the MAC (Wi-Fi) addresses broadcast by customers' mobile phones. This allows stores to do what websites do all the time: tweak their configuration, pricing, purchasing and the like in response to real-time analytics — instead of just eyeballing what works. Nomi anonymized the data it collected through a one-way hash, so that retailers couldn't track specific individuals. Recognizing that some customers might still object, even to "anonymized" tracking, Nomi allowed anyone to opt-out of all Nomi tracking on its website.

Nomi's website promised to "[a]lways allow consumers to opt-out of Nomi's service on its website as well as at any retailer using Nomi's technology." But Nomi never actually offered an opt-out in-store — and Nomi's retail partners never posted notices in their stores to inform consumers that they were using Nomi, or that they could exercise the opt-out. Instead of suing the retailers for failing to disclose this data collection, the FTC alleged that Nomi had committed two deceptive practices:

- Count I (Express Claim): Failing to offer an in-store opt-out
- Count II (Implied Claim): Failing to offer in-store notices

Nomi marks the first time the FTC has made such claims regarding in-store tracking, or regarding an alleged failure to provide an in-store opt-out. Because the case was settled out of court, the majority did little to explain its analysis. In fact, both claims stand on shaky legal ground.

Materiality under the FTC's Deception Policy Statement

In theory, the FTC's Section 5 authority is supposed to be used to protect consumers by reaching conduct in interstate commerce not sufficiently handled by common law and contract remedies.[3] In the 1970s, a broadly worded Supreme Court decision combined with Naderite criticism of the agency inspired a frenzy of activity.[4] That, in turn, provoked a backlash from the deregulatory Carter-era Democrats. Congress forced the agency to set boundaries on both unfairness (1980)[5] and deception (1983).[6] But the FTC has effectively circumvented those constraints little by little through enforcement actions such as that against Nomi.[7]

---

[3] *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590-606 (2013).

[4] *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (speech given at the Marketing and Public Policy Conference, May 30, 2003), *available at* https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection; FTC v. Sperry & Hutchinson Trading Stamp Co., 405 U.S. 233 (1972).

[5] *See* Letter from Michael Pertschuk, Chairman, FTC, to Hon. Wendell H. Ford, Chairman, Senate Comm. on Commerce, Science and Transportation (Dec. 17, 1980), *appended to* International Harvester Co., 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[6] *See* Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983), *appended to* In re Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)

The 1983 Deception Policy Statement (DPS) requires the FTC to show that:

1. There is a representation, omission or practice that is likely to **mislead** the consumer;
2. A consumer's **interpretation** of the representation, omission, or practice is considered **reasonable** under the circumstances; and
3. The misleading representation, omission, or practice is **material**.[8]

Back in 1965, in *Colgate-Palmolive*, the Supreme Court had essentially abolished the materiality requirement previously recognized by the FTC, allowing the FTC to presume that any statement or omission that a reasonable person would find misleading was deceptive[9] — just as the Court's 1972 decision in *Sperry v. Hutchison* essentially deleted the injury requirement of unfairness.[10] The 1983 DPS was, like the 1980 Unfairness Policy Statement, a compromise — walking the Commission back from its unconstrained activism of the 1970s, but not going as far in constraining the agency as some of its critics wanted.

In Congressional testimony in 1982, FTC Chairman Miller proposed that materiality should require some proof of consumer harm, which would have made deception harder to establish and more like the common law (*e.g.*, the torts of deceit or fraud).[11] In the end, the DPS said instead that materiality was a *proxy* for harm, which generally the FTC would not separately need to prove: "if the practice is material, [then] consumer injury is likely, because consumers are likely to have chosen differently but for the deception."[12] This allowed the FTC to retain authority over misleading practices that would not necessarily violate any common law standard.[13]

At the same time, the FTC retained *some* of the prior presumption of materiality, but the DPS narrowed the scope of the presumption: "[i]n many instances, materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary."[14] The DPS left somewhat unclear just how broad the remaining presumption should be. It left even less clear how one could rebut that presumption, and how conflicting evidence about materiality should be resolved without the presumption.

(decision & order), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception [hereinafter "Deception Policy Statement" or "DPS"].

[7] *See* FTC, *Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt-out Choices* (Apr. 23, 2015) (press release), https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.

[8] *See* Deception Policy Statement, *supra* note 6, at 175-76.

[9] FTC v. Colgate-Palmolive Co. 380 U.S. 374 (1965); *see generally* Jef I. Richards & Ivan L. Preston, *Proving & Disproving Materiality of Deceptive Advertising Claims*, 11(2) J. PUB. POL'Y & MARKETING 45, 49 (1992).

[10] *See* FTC v. Sperry & Hutchinson Trading Stamp Co., 405 U.S. 233 (1972).

[11] *See* Richards & Preston, *supra* note 9, at 49-50.

[12] Deception Policy Statement, *supra* note 6, at 176.

[13] *See* Richards & Preston, *supra* note 9, at 49-50.

[14] Deception Policy Statement, *supra* note 6, at 176.

The DPS says that "express claims are material," and quotes the Supreme Court's landmark 1980 *Central Hudson* decision (which extended First Amendment protection to commercial speech for the first time):

> In the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising.[15]

The Court was talking about the societal value of the speech, but the FTC extended the logic: an advertiser's willingness to make an express claim became a proxy for materiality, which is *itself* a proxy for harm.

In traditional advertising, this "express claim => materiality => harm" formulation may make sense: who knows better than the advertiser whether a claim is likely to influence consumer behavior (*i.e.*, be "material")? But this presumption doesn't *always* make sense, as the Supreme Court noted. Unfortunately, the FTC seems to have forgotten this caveat, and has slipped back into a presumption of materiality that is both sweeping and, in practice, not rebuttable — just as in the pre-1983 era.

The DPS *does* require evidence when claims are merely implied.[16] The FTC must prove either that a seller *intended* to convey an implied claim,[17] or, if the FTC cannot prove intent, it must instead prove materiality, and cannot rely on the presumption.[18]

The DPS extends the presumption of materiality to several other scenarios, such as (i) misleading information or omissions ordinary consumers need to evaluate a product or service or (ii) omissions with which the reasonable consumer would be concerned, such as health or safety.[19] In both cases, though, the FTC must at least present evidence that the omitted information is "necessary" to ordinary consumers or of "concern" to reasonable consumers before the materiality presumption attaches.

Finally, even where the DPS allows the FTC to presume materiality, it makes clear that, contrary to the 1965–1983 period, that presumption is rebuttable: "The Commission will always consider relevant and competent evidence offered to rebut presumptions of materiality."[20] In few

---

[15] *Id.* at 189 n.49 (quoting Central Hudson Gas & Electric Co. v. PSC, 447 U.S. 557, 567 (1980)).

[16] Deception Policy Statement, *supra* note 6, at 190 ("Similarly, when evidence exists that a seller intended to make an implied claim, the Commission will infer materiality.").

[17] *See id.*

[18] *See id.* at 191.

[19] *See id.* at 189 ("Where the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false"); *id.* at 190 ("The Commission also considers claims or omissions material if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned.").

[20] *Id.* at 189 n.47.

cases, however, has the Commission actually weighed conflicting evidence,[21] and never has the FTC published guidance on what evidence might qualify as "relevant or competent" to rebut the presumption of materiality. And those cases that do exist concern traditional marketing claims, not the kinds of novel fact patterns created by cutting-edge companies like Nomi.

Thus, lawyers advising clients facing a deception enforcement action, or trying to avoid one in the future, must rely primarily on complaints, consent decrees, and agency statements to attempt to predict how the FTC might weigh materiality. Unfortunately, the FTC has, under this Administration, effectively stopped issuing closing letters to explain why it decided *not* to bring an enforcement action,[22] so there is essentially no body of law showing how the FTC decides *not* to bring an enforcement action regarding a claim (or omission) that was misleading but that the FTC decided was *not* actually material. Thus, it is hardly surprising that companies settle essentially all cases the FTC brings — which further compounds the problem, by denying other practitioners litigated cases where the issue has been explored.[23]

Applying the Deception Policy Statement to *Nomi*

Applying the DPS framework to *Nomi* requires first assessing whether the presumption of materiality should apply.

Nomi's Express Promises: The Presumption of Materiality Was Misapplied

Count I of the FTC's *Nomi* complaint rests on applying the presumption of materiality to the following express claim made in the privacy policy on Nomi's website:

> Nomi pledges to… Always allow consumers to opt-out of Nomi's service on its website as well as at any retailer using Nomi's technology.[24]

Everyone agrees that Nomi complied with the first half of this promise by allowing consumers to opt-out on its website.[25] But the FTC alleges that the second half was deceptive because:

---

[21] *See, e.g.*, Novartis Corp. v. FTC, 223 F.3d 783 (D.C. Cir. 2000); Kraft Inc. v. FTC, 970 F.3d 311 (7th Cir. 1992).

[22] *See* Geoffrey A. Manne & Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security* 4 (ICLE Working Paper), *available at* http://bit.ly/1byrNS2 ("In order to get a better handle on the universe of [data security] cases at the FTC that didn't result in settlements, we filed a FOIA request with the agency. It showed only seven closing letters and three emails closing investigations without bringing a case.").

[23] *See generally id.*; Berin Szoka, *Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection "Case Law"* (2014 TPRC Conference Paper, Aug. 22, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418572.

[24] In the Matter of Nomi Technologies, Inc., Complaint, at ¶12 (Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf [hereinafter "Nomi Complaint"].

[25] *See* In the Matter of Nomi Technologies, Inc., Statement of Chairwoman Ramirez, Commissioner Brill, and Commissioner McSweeny, at 1-2 (Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/638351/150423nomicommissionstatement.pdf [hereinafter "Majority Statement"]; In the Matter of Nomi Technologies, Inc., Dissenting Statement of Commissioner Maureen K. Ohlhausen, at 1 (Apr. 23, 2015), *available at*

1. Nomi failed to make sure that each retailer in fact offered an in-store opt-out mechanism; or
2. Nomi failed to identify the retailers that used its technology (or failed to cause the retailers to identify themselves).[26]

The first claim appears straightforward: Nomi did not, in fact, offer an in-store opt-out mechanism, in violation of its express promise to do so.[27] For the majority, this is the end of the matter: even though the website portion of the promise was fulfilled, Nomi's failure to comply with the in-store promise portion amounts to an actionable deception.

But bifurcating the privacy policy in this way seems to violate the DPS's requirement that all statements be evaluated in context:

> [T]he Commission will evaluate the entire advertisement, transaction, or course of dealing in determining how reasonable consumers are likely to respond. Thus, in advertising the Commission will examine "the entire mosaic, rather than each tile separately."[28]

Courts have suggested much the same thing:

> [T]he tendency of the advertising to deceive must be judged by viewing it as a whole, without emphasizing isolated words or phrases apart from their context.[29]

The majority dodges the key question: whether the evidence that Nomi accurately promised a *website* opt-out, and that consumers could (and did) opt-out using the website, rebuts the presumption that the inaccurate, in-store opt-out portion of the statement was material, and sufficient to render the statement *as a whole* deceptive. As Stanford Law Professor Richard Craswell has pointed out:

> [S]ome method will have to be devised for determining when a statement that accurately informs in one respect while misleading the listener in another should properly be regarded as deceptive. This determination can be made without any trade-offs only if we are willing to say that any deception of the listener is enough to label the

---

https://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf [hereinafter "Ohlhausen Dissent"]; In the Matter of Nomi Technologies, Inc., Dissenting Statement of Commissioner Joshua D. Wright, at 3 (Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf [hereinafter, "Wright Dissent"].

[26] *Cf.* Nomi Complaint, *supra* note 24, at ¶14 ("Nomi represented, directly or indirectly, expressly or by implication, that consumers could opt-out of Nomi's Listen service at retail locations using this service"); *id.* at ¶16 ("Nomi represented, directly or indirectly, expressly or by implication, that consumers would be given notice when a retail location was utilizing Nomi's Listen service").

[27] *Id.* at ¶15.

[28] Deception Policy Statement, supra note 6, at 183 n.31 (quoting FTC v. Sterling Drug, 317 F.2d 669, 674 (2d Cir. 1963)).

[29] Beneficial Corp. v. FTC, 542 F.2d 611, 617 (3d Cir. 1976).

> statement itself deceptive, analogous to holding that an advertisement should be deemed deceptive if it deceives even a single consumer.[30]

Here, as Commissioner Wright argues,

> the Commission failed to discharge its commitment to duly consider relevant and competent evidence that squarely rebuts the presumption that Nomi's failure to implement an additional, retail-level opt-out was material to consumers. In other words, the Commission neglects to take into account evidence demonstrating consumers would not "have chosen differently" but for the allegedly deceptive representation.[31]

As Commissioner Wright points out, the available evidence suggests that consumers were apparently not particularly affected by the inaccurate portion of the statement. He cites evidence that 3.8% of consumers used Nomi's website to opt-out of data collection — a number considerably higher than the less than 1% who opt-out from data collection online more generally.[32] From this, Wright notes, it may be inferred that the consumers who read Nomi's policy and who cared to avoid its technology likely opted-out at the website.[33]

It is of course a valid question whether, even in context, the inaccurate statement amounted to a material deception, and whether the evidence offered by Commissioner Wright was sufficient to rebut the presumption of materiality. Nevertheless, the majority's *approach* to answering those questions (*i.e.*, dismissing or ignoring them) and weighing the evidence (*i.e.*, failing to) betrays the majority's implicit rejection of the DPS's admonishment that context and contrary evidence are essential — and the DPS's promise that "The Commission will always consider relevant and competent evidence offered to rebut presumptions of materiality."[34]

The majority *does* offer some theories as to why the inaccurate in-store opt-out statement might have mattered, even to consumers confronted with the additional, website opt-out. Nonetheless, it essentially rejects the idea that there could be a valid trade-off. Instead, the majority seems content to assert that if *any* consumer might have been misled by the in-store opt-out promise, the statement is material. In reality, what the DPS requires is a weighing of the importance of the inaccurate language against the truthfulness of the statement taken as a whole. In other words, it is not enough to suggest (without evidence, of course, but only supposition) that the inaccurate language could have misled some consumers; the DPS requires a showing that the

---

[30] Richard Craswell, Regulating Deceptive Advertising: The Role of Cost-Benefit Analysis, 64 S. CAL. L. REV. 549, 594 (1991).

[31] Wright Dissent, *supra* note 25, at 3.

[32] *Id.* at 3, 4.

[33] *Id.*

[34] Deception Policy Statement, *supra* note 6, at 189 n.47.

entire statement, taken as a whole, *tended* to mislead "a consumer acting reasonably in the circumstances."[35] This is quite a different assessment, and one that the majority fails to undertake.

Nomi's (Alleged) Implied Promise: No Presumption of Materiality

In addition to rejecting Commissioner Wright's evidentiary claims regarding Nomi's express promises, the majority attempts to bolster its case by asserting that:

> the express promise of an in-store opt-out necessarily makes a second, implied promise: that retailers using Nomi's service would notify consumers that the service was in use. This promise was also false. Nomi did not require its clients to provide such a notice. To our knowledge, no retailer provided such a notice on its own.[36]

As noted above, under the DPS an implied promise merits the presumption of materiality only when there is proof that the implied promise was *intended* by the speaker.[37] In the absence of such proof, the FTC would (at least if it were before a court) have to prove the materiality of the alleged implied promise. In other words, for an implied promise to be deemed material (and thus deceptive) under the DPS, the FTC must adduce *some* proof: either that it was, in fact, *intended*, or that it was, in fact, *material*.

The FTC Failed to Prove Nomi's Intent to Make the Implied Promise of In-Store Notification

The majority attempts to "prove" that Nomi intended to make the implied promise by asserting that such a promise was necessary to the express promise of an in-store opt-out.[38]

But why is such a promise "necessarily" implied by Nomi's statement? One can readily see that in-store opt-out would be *easier* for consumers if stores posted signs or otherwise conspicuously notified their customers that Nomi's technology was in use. But Nomi doesn't make any promise as to the particular mechanism by which in-store opt-out would be available.

It would seem to eviscerate the word "proof" if proof of intent could be satisfied here by a simple assertion of "necessity" when *any* other interpretation is possible. Something more convincing *must* be required — whether evidence of actual intent (*e.g.*, "hot docs" clearly stating the intent of the company) or evidence undermining the other possible interpretations (*e.g.*, evidence that no other company *ever* used such language without intending or assuming that notice was required).

But the FTC offers no such evidence here, and other interpretations *are* possible.

---

[35] *Id.* at ("If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group.)

[36] Majority Statement, *supra* note 25, at 1.

[37] *See* Deception Policy Statement, *supra* note 6, at 190.

[38] *See* Majority Statement, *supra* note 25, at 1 ("Moreover, the express promise of an in-store opt-out necessarily makes a second, implied promise").

For example, Nomi's technology uses the MAC addresses broadcast by consumers' smartphone Wi-Fi interfaces to track consumers' movements through retail stores.[39] This necessarily means that every tracked consumer was carrying a Wi-Fi equipped mobile device while in-store. It is undisputed that Nomi's website offered the promised opt-out.[40] Thus, its additional promise to make opt-out available "at any retailer using Nomi's technology" could conceivably have been fulfilled by ensuring that the stores' Wi-Fi was connected to the Internet and potentially accessible to consumers — so that consumers could access the website opt-out from their phones while in the store (if they could not already do so from their mobile data connections. If so, consumers planning to avail themselves of in-store opt-out were no more deceived by the absence of in-store notification than were consumers who opted-out at Nomi's website — a claim the majority doesn't make.[41] In either case, they wouldn't have known — or needed to know — which stores used Nomi to exercise the website opt-out.

But even if we assume that the promised in-store opt-out could only reasonably have been assumed to use a different mechanism than the website opt-out, it still doesn't *require* in-store notification that Nomi's technology was in use. Again, while such notification would have made opt-out *easier*, it is not clear that a consumer, having read Nomi's simple, one-page privacy policy, couldn't have been reasonably expected to assume that *every* store might be using Nomi's technology and obligated to ask a store employee if he wanted to use the retail opt-out. The opt-out itself does, after all, require the consumer to engage in an affirmative act to avoid tracking. In fact, in a world in which various forms of tracking, monitoring and surveillance are effectively ubiquitous (not least because government surveillance has made this world a reality), such an assumption might be fairly realistic.

If this harsh truth seems unacceptable, note two things. First, the consumer at issue was not powerless: he was given an easy, comprehensive opt-out, which he could exercise without any special notification and at trivial cost. Second, this case does nothing to avoid the lack of in-store notification — indeed, it probably makes it more likely, by discouraging disclosure generally, as explained below. The FTC could, in theory, have brought an unfairness case against Nomi for failing to disclose its collection to all tracked consumers, or either a deception or unfairness case against retailers for failing to notify their customers that they were being tracked. Any of these cases would have dealt directly with what would seem to be the source of the FTC majority's real discomfort: tracking without conspicuous notification to all consumers. But the Commission brought no such cases. Instead it seems content to try to extend its limited deception authority beyond its legal limits in a misguided effort to locate a generalized disclosure requirement for data collection and tracking activity in that authority.

In recent years, the FTC has brought a series of cases aimed at mandating disclosure and/or dictating how disclosure must formatted, configured or delivered — without regard for countervailing economic considerations, and with little humility about the FTC's ability to create effec-

---

[39] Nomi Complaint, *supra* note 24, at ¶4.

[40] *Id.* at ¶11.

[41] *See* Majority Statement, *supra* note 25, at 2-3.

tive user interfaces from the top down.[42] The FTC considerably stepped up this approach with its recent settlements against Apple, Google, and Amazon regarding precisely how they configured their online stores to prevent children from making app purchases without their parents' authorization.[43] Taken together with *Nomi,* it is difficult not to see in this set of cases an effort by the FTC to bootstrap into its deception and unfairness authority an ability to mandate some form of conspicuous notification for offline consumer tracking — ideally through notifications "pushed" to consumers' mobile devices in real time to notify them of potential tracking.

While that may (or may not) be a desirable policy, it is not one that the FTC's Section 5 authority permits the FTC to mandate. Indeed, the fact that Section 5 does *not* confer such broad authority is a key reason why FTC has sought the authority to mandate specific forms of disclosure as part of "comprehensive baseline privacy legislation" under Democratic Administrations (in 2000, and again more recently).

Only by stretching Section 5 across a series of un-adjudicated settlements can the FTC possibly create such a legal disclosure requirement. Whatever the merits of such an outcome, contorting Section 5 to reach it creates a host of problems. The constraints of the DPS (like those of the UPS and Section 5(n)) are not simply legalistic obstacles to be overcome: they help to ensure that the FTC doesn't run roughshod over innovative technologies, micro-manage design choices, and unduly intrude on companies' reasonable economic decision-making. To be sure, there may be perfectly valid constraints on these imposed by the FTC. But the FTC's apparent effort to escape *any* constraints on its own authority to dictate even the most trivial details of disclosures, privacy policies and notifications (particularly when data collection is involved) will not serve consumers well on balance.[44]

The FTC Failed to Prove that Nomi's (Alleged) Implied Promise of In-Store Notification Was Material

In the absence of proof of intent (and even if it *is* present, given the DPS's requirement that the FTC "always consider relevant and competent evidence offered to rebut presumptions of materiality"), the FTC must prove that an implied promise was material.[45] Here again the majority fails.

---

[42] *See* Solove & Hartzog, *supra* note 3, at 658-61 (and enforcement actions cited therein).

[43] *See* In the Matter of Apple, Inc., Complaint, (Jan. 15, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf; In the Matter of Google, Inc., Complaint, (Sept. 4, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140904googleplaycmpt.pdf; FTC v. Amazon.com, Inc., Complaint, (W.D. Wash., Jul. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140710amazoncmpt1.pdf.

[44] *See* Geoffrey Manne & Ben Sperry, *Debunking the Myth of a Data Barrier to Entry for Online Services*, TRUTH ON THE MARKET (Mar. 26, 2015), http://truthonthemarket.com/2015/03/26/debunking-the-myth-of-a-data-barrier-to-entry-for-online-services/.

[45] *See* Deception Policy Statement, *supra* note 6, at 191 ("Where the Commission cannot find materiality based on the above analysis, the Commission may require evidence that the claim or omission is likely to be considered important by consumers. This evidence can be the fact the product or service with the feature represented

As the DPS notes:

> Because this presumption [of materiality for express statements] is absent for some implied claims, the Commission will take special caution to ensure materiality exists in such cases.[46]

The majority showed no such caution and adduced no such evidence to support its presumption of materiality for the implied statement.[47] Moreover, the violation of the asserted implied promise of in-store notification is logically unlikely to be material because, whatever precisely Nomi's statement reasonably *implied*, it *expressly* required some affirmative action by the consumer to opt-out.

The DPS states:

> In cases of implied claims, the Commission will often be able to determine meaning through an examination of the representation itself, including an evaluation of such factors as the entire document, the juxtaposition of various phrases in the document, the nature of the claim, and the nature of the transactions.[48]

The majority asserts that notice of in-store tracking at each location was material because

> consumers visiting stores that used Nomi's services would have reasonably concluded, in the absence of signage and the promised opt-outs, that these stores did *not* use Nomi's services. Nomi's express representations regarding how consumers may opt-out of its location tracking services go to the very heart of consumers' ability to make decisions about whether to participate in these services. Thus, we have ample reason to believe that Nomi's opt-out representations were material.[49]

But the relevant knowledge required for consumers to have the "ability to make decisions about whether to participate in these services" isn't whether Nomi's services were in use at any particular location; it's whether the consumer has, in fact, made an effective choice whether to participate. In other words, what matters is a consumer's knowledge of whether he or she actually opted-out. And *every consumer* who read the privacy policy had that notice.

If consumers saw Nomi's website privacy policy and *still* went shopping knowing that they hadn't ever taken the affirmative step of opting-out (whether online or in-store), they weren't "deceived" by the absence of in-store notifications.

Again, to some, this might sound harsh: "You're on notice now that the world has changed, so *caveat emptor*!" But remember that any consumer who saw the notice was empowered to opt-out

---

costs more than an otherwise comparable product without the feature, a reliable survey of consumers, or credible testimony").

[46] *Id.* at 189 n. 48.

[47] *See* Majority Statement, *supra* note 25, at 2-3.

[48] *See* Deception Policy Statement, *supra* note 6, at 177.

[49] Majority Statement, *supra* note 25, at 2.

quite easily. And the record contains no evidence that, once put on notice, even a single consumer tried to opt-out in-store and was thwarted.[50]

Nothing Nomi did (or didn't do) with respect to notice necessarily affected consumers' failure to affirmatively opt-out if they didn't do so on the website — unless the claim is that they all *forgot* about the tracking once they left the website without opting-out, and the absence of conspicuous notices to remind them caused them to act against their intentions.

But the majority doesn't make this argument. And it would be difficult to square with the majority's assertion (which it is forced to make in order to counter Commissioner Wright's argument that the website opt-out alone was sufficient) that the harmed consumers were particularly privacy-sensitive:

> Consumers who read the Nomi privacy statement would likely have been privacy-sensitive, and claims about how and when they could opt-out would likely have especially mattered to them.[51]

The majority goes on to hypothesize several scenarios in which these privacy-sensitive consumers might still have chosen not to opt-out on the website:

> Some of those consumers could reasonably have decided not to share their MAC address with an unfamiliar company in order to opt-out of tracking, as the website-based opt-out required. Instead, those consumers may reasonably have decided to wait to see if stores they patronized actually used Nomi's services and opt-out then. Or they may have decided that they would simply not patronize stores that use Nomi's services, so that they could effectively "vote with their feet" rather than exercising the opt-out choice. Or consumers may simply have found it inconvenient to opt-out at the moment they were viewing Nomi's privacy policy, and decided to opt-out later.[52]

All but the first of these are indeed plausible. (The first isn't plausible because even if Nomi had offered an opt-out in-store, consumers presumably would *still* have had to provide a MAC address. At most, perhaps some consumers might have felt somewhat more comfortable providing a MAC address in-person rather than online, but this is highly speculative — the kind of evidence that perhaps the Commission might have weighed among other evidence, but hardly an argument for insisting on the presumption of materiality, which avoids *any* evidentiary inquiry.)

But while in-store notices might have made it *easier* for consumers who preferred to opt-out in-store, nothing changes the fact that, as long as they *didn't* opt-out, every consumer who read Nomi's website policy and continued to shop nonetheless was on notice that they might be tracked.

---

[50] *Cf.* Nomi Complaint, *supra* note 24, at ¶13.

[51] Majority Statement, *supra* note 25, at 2.

[52] *Id.*

The closest the majority comes to making a viable argument for the materiality of the implied promise to provide in-store notices is its claim that "consumers visiting stores that used Nomi's services would have reasonably concluded, in the absence of signage and the promised opt-outs, that these stores did *not* use Nomi's services."[53]

Unfortunately for the majority, however, in the absence of proof that Nomi intended to make such a (false) promise (presumably, it would be to induce consumers to infer that stores without notices did not use Nomi's services), the materiality of such a promise can't be presumed. And a mere statement by three FTC commissioners asserting that consumers "would have reasonably" interpreted the absence of notices to mean Nomi's services weren't present is insufficient — particularly with respect to nascent technology and the rapidly evolving world of consumer data collection and privacy.

As even Dan Solove and Woody Hartzog, defenders of the FTC's "common law of settlements" and the Commission's general approach to privacy and data security, point out:

> Social science research is revealing that consumers do not read or understand privacy policies, are heavily influenced by the way choices are framed, and harbor many pre-existing assumptions that are incorrect. For example, according to one study, "64% [of the people surveyed] do not know [or falsely believed] that a supermarket is allowed to sell other companies information about what they buy" and that 75% falsely believe that when "a website has a privacy policy, it means the site will not share my information with other websites or companies."[54]

There is much we don't know about consumers' assumptions (and their reasonableness) regarding privacy policies and their implications. Assuming without evidence that consumers would have reasonably interpreted the absence of notices to mean no tracking was present is an unwarranted leap.

The FTC Failed to Adequately Consider Factors that Rebut the Presumption of Materiality

The Deception Policy Statement carefully quotes *Central Hudson*, including this critical proviso:

> *[I]n the absence of factors that would distort the decision to advertise*, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising.[55]

In *Nomi* the majority fails to consider those factors, which increasingly distinguish the marketing claims of the 1980s from today's privacy policies — not just in this case, but across the privacy and data security cases brought by the agency.

---

[53] *Id.*

[54] Solove & Hartzog, *supra* note 3, at 667.

[55] *See* Deception Policy Statement, *supra* note 6, at 189 n.49 (quoting Central Hudson Gas & Electric Co. v. PSC, 447 U.S. 557, 567 (1980)).

For materiality to make sense as a proxy for consumer harm, it must be reasonable to assume that an express statement in fact induced (or was likely to induce) harmful actions. That may be the case when advertising states that a product contains no nuts, say — a clear attempt to induce even those consumers who are allergic to nuts to purchase the product. It is reasonable to assume that such a statement, if false, could cause harm. Importantly, the harm would be caused by the action intended to be caused by the statement: purchase and consumption of the product, even by consumers who are allergic to nuts.

But several factors distinguish statements like the Nomi's privacy policy from traditional marketing claims. First, in this case (and others like it), refuting or confirming the alleged misrepresentation is wholly within the consumer's control. If, after viewing the privacy policy, a consumer shops anywhere without affirmatively opting-out, the consumer knows he hasn't opted-out; he hasn't been deceived and he's in full awareness of all the relevant facts. He doesn't have to *know* whether any particular store uses Nomi's services or not to know with certainty that he hasn't opted-out.

In other words, absent an affirmative opt-out by the consumer, it's impossible to assume that the implied (or express, for that matter) statement was material to the consumer's choice and thus that it caused any harm. The intervening step — opt-out by the consumer — can't just be ignored. For consumers who chose to shop without opting-out (or trying to opt-out), Nomi's inaccurate statement simply can't be presumed to have been material without proof.

Second, the choice at issue here is not the consumption of a product; it is the exercise of an opt-out. To the extent that the ability to opt-out from tracking may be an important characteristic of a product being consumed, it is either a characteristic of the product that *retailers* are purchasing from Nomi, or else it is a characteristic of the product that consumers are purchasing from *retailers*. It makes no difference that the opt-out *mechanism* may be offered to consumers directly by Nomi. The decision to consume a retailer's product and the decision to track consumers (whether or not they can opt-out of such tracking) are not part of the same "product," and they are not made by the same party. The inclusion of an opt-out gives consumers some influence over the retailer's decision (or ability) to track, but whether the efficacy of that influence comports with a retailer's expectations is a contractual matter between Nomi and the retailer. This presents a dramatically different dynamic, and different set of incentives, than the marketing statements traditionally at issue in deception cases.

Third, and related, remember that the basis for presuming that express statements are material is that, if the marketer invests in an advertisement, it expects that advertisement to sell more of its products. The presumption rests on the marketer's self-interest: in legal terms, the marketer is *estopped* from claiming, after the fact, that a statement that it made precisely because it was material to consumers was not, in fact, material after all.

But with privacy policies, any correlation between the company's self-interested calculation of relevance at the time it made the claim and the actual materiality to consumers can be, and likely is, far more attenuated. Some claims about privacy might well be equivalent to traditional marketing claims (such as an ad touting the privacy features of a product over one's competitors). But in general, it cannot be presumed that all privacy policies are intended to convince consumers to use the product — and certainly not to persuade them to opt-out from the product,

the very opposite of what the company wants! Privacy policies may sometimes, in fact, be required by law,[56] and their contents reflect considerable pressure from the FTC itself, among other government actors, to disclose more about a company's privacy practices. Finally, privacy policies, unlike ads, generally do not reflect the investment of money into a campaign intended to persuade consumers.

These points, combined with the FTC majority's theoretical (rather than evidence-based) rejection of the evidence adduced by Commissioner Wright that consumers used the website opt-out at a greater-than-typical rate, render the assumption of materiality for *both* the express and implied statements tenuous. These are all important issues that the FTC *should* have addressed — and likely would have *had* to address, had it taken the case to court, instead of simply settling it.

What *Nomi* Means and What to Do About It

In effect, the *Nomi* settlement seems to stand for the disturbing proposition that the presumption that an express statement is material can *never* be rebutted — not even by evidence that it didn't change, and couldn't have changed, consumers' choices. As Commissioner Ohlhausen says, this amounts to a strict liability standard, without any need to establish either materiality or harm — precisely the unconstrained 1965 version of deception rejected by the Commission in the Deception Policy Statement.[57]

In summary, we believe the Commission is committing four legal errors in its application of the Deception Policy Statement:

1. Failing to adequately weigh evidence that the materiality presumption has been rebutted;
2. Treating claims in isolation, rather than in their full context;
3. Assuming, without proof, that Nomi intended to make the implied claim about in-store notices; and
4. Similarly, even when the presumption does not apply (such as for an implied claim that the FTC has not proven the defendant intended to make), failing to offer sufficient evidence to prove materiality.

Had this case gone to a court, we believe a court might well have rejected these arguments, or the FTC might not have made these arguments in the first place for fear that a court would

---

[56] CAL. BUS. & PROF. CODE §§22575-79, *available at* http://leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579. Although Nomi didn't "collect[] personally identifiable information through the Web site or online service," as the California law requires, it's not much of a stretch to assume that a young technology company like Nomi might post such a policy out of an abundance of caution. And California is in the process of amending its law to apply to all data collection. Proposed laws like the proposed White House Privacy Bill, moreover require such disclosures more broadly. *See* Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, THE WHITE HOUSE (Feb. 27, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[57] Ohlhausen Dissent, *supra* note 25, at 1 ("we should not apply a de facto strict liability approach to a young company that attempted to go above and beyond its legal obligation to protect consumers but, in so doing, erred without benefiting itself").

reject them — but it is difficult to say given the lack of relevant adjudicated precedent, and the general tendency of courts to defer to administrative agencies in such contexts. Both because litigation on these issues is unlikely and because, even if litigation does occur, it may not correct these errors, we believe that Congress (or the FTC itself) must require the FTC to bring its approach in line with the DPS.

In addition, while the FTC may be accurately reading the plain text of the DPS ("the Commission presumes that express claims are material"), we question whether it makes sense to extend the presumption to express statements that differ fundamentally from the type of claims with which the Commission was primarily concerned back in 1983, such as in privacy policies like Nomi's, for all the reasons explained above.

Of course, it is true that, even in 1983, the Commission had long applied deception not only to marketing claims in advertisements, but also to warranties and contracts — and, presumably, when the DPS "presumes that express claims are material," it includes claims in these documents as well as in advertisements. Those documents might resemble today's privacy policies or terms of service in some respects: many are lengthy and legalistic. But on the whole, they are significantly different from privacy policies like Nomi's in the key respect that matters: they are, like advertisements, intended to help convince consumers to buy a product.

In 1983, the Commission did not have to grapple with this question because it could safely assume that all express statements were essentially similar: whatever their length or format, they reflected the same basic alignment of incentives. Today, the world of express statements made by companies has grown considerably. It may be time to consider clarifying whether the presumption of materiality applies to these statements at all, or only to express statements made to persuade a consumer to purchase (or consume) a product. Some privacy policies might well qualify for the presumption, like those of consumer-facing services, but Nomi's likely would not. Of course, a privacy policy like Nomi's could well still be material, but the FTC would bear *some* burden of proving this.

To a large degree, this concern could be addressed simply by ensuring that the FTC made good on the DPS's promise to "always consider relevant and competent evidence offered to rebut presumptions of materiality."[58] This would not entirely correct the problem, of course; the burden would remain upon the defendant to rebut the presumption. And in some of those cases, it may be the FTC that should bear the burden for all the reasons expressed above. But it would at least be a significant improvement over the status quo.

Finally, like Commission Ohlhausen, we question the FTC's use of its prosecutorial discretion: it is difficult to see how this case will actually make consumers better off. Yet we recognize that, as a legal matter, the FTC enjoys broad deference on this point. Indeed, the FTC Act does not actually specify *any* legal standard the FTC must satisfy before settling a case (which itself suggests that the Congress that took such great pains to constrain the FTC's rulemaking authority

---

[58] Deception Policy Statement, *supra* note 6, at 189 n.47.

with the Magnuson-Moss Act of 1980 and to force the FTC to narrow its understanding of unfairness would be shocked to discover that the FTC today operates entirely by settlement).

By their own terms, the FTC's settlements claim only to satisfy Section 5(b), which requires only that the decision to bring an enforcement action (not a settlement) be supported by (i) "reason to believe" a violation of the Act occurred and (ii) the Commission's belief that an investigation would be in the public interest.[59] As Commissioner Wright argues, "that threshold should be at least as high as for bringing the initial complaint."[60] We agree — but so long as there is no clear standard, any three Commissioners will retain broad discretion to settle cases that may have highly questionable benefits for consumers and may, over time, skew the FTC's understanding of its guiding doctrines.

What to Do about These Problems: Potential Reforms

In principle, the Commission *could* make significant improvements on each of these three problems. Yet the agency has had 32 years to clarify materiality and has failed to do so; indeed, the Commission has actually reverted to a less sensible approach. And the "common law of consent decrees" problem has greatly accelerated in the last 18 or so years as the Commission has applied both deception and unfairness in novel ways that push the boundaries of both policy statements — all without effective judicial oversight.

We believe that real, lasting reform will likely require Congressional intervention — and that Congress has essentially three options:

1. Require the FTC to issue a policy statement on materiality, within certain parameters;
2. Constrain the FTC by statute, akin to adding Section 5(n) in 1994, and
    a. Attempt to craft limiting principles itself; or
    b. Outsource the task of deciding on limits to a Privacy Law Modernization Commission, such as we have previously proposed, and then implement the recommendation in legislation; and/or
3. Focus on process reforms that will make the FTC more likely to have to litigate in court — so that the courts will be in a position to insist that the FTC better explain its analysis.

We believe all three may be necessary, but that the second two are especially critical in the long term: Commissioners will come and go but the FTC should remain laser-focused on consumer injury.

A New Policy Statement on Materiality?

Congress could ask or even require the FTC to issue a Policy Statement on Materiality — or, perhaps "guidelines" — making clear that these are intended to elaborate upon and clarify, not supersede, the Deception Policy Statement. This could mark a substantial improvement over the

---

[59] 45 U.S.C. § 45(b).

[60] Wright Dissent, *supra* note 25, at 2.

status quo, in much the same way that, at least for a time, the UPS and DPS served to constrain the FTC's uses of unfairness and deception.

In short, a new policy statement would likely be better than nothing — if it actually happened. Given the refusal of Chairwoman Ramirez even to entertain the proposals by Commissioners Wright and Ohlhausen for a Policy Statement on Unfair Methods of Competition (the third major area of the FTC's Section 5 authority, which the FTC has never defined and which simply was not at issue in the 1970s/80s fights over consumer protection[61]), it seems likely that significant political pressure would have to be exerted to force the FTC to do something it does not want to do — effort that we believe would be better spent on legislative solutions.

But, in addition, we see several obvious drawbacks to this approach:

1. **The FTC can revoke a policy statement at any time** without any notice or public input.[62] This is precisely what the FTC did in 2012, summarily revoking a policy the Commission's 2003 Policy Statement on Monetary Equitable Remedies in Competition Cases (better known as the "Disgorgement Policy Statement") — over the loud dissent of Commission Ohlhausen.[63]
2. Even while in effect, **policy statements aren't actually binding upon the FTC** — as explained below.
3. **The FTC has little incentive to constrain its discretion**, so the any policy statement it did produce would likely only formalize its current, expansive views of materiality.

Putting the Deception and Unfairness Policy Statements in Context

Crafting effective legislation requires understanding the historical perspective of both the Deception and Unfairness Policy Statements, which the Commission offered to forestall further legislative reforms (as Congress had curtailed FTC rulemaking earlier in 1980).[64] It's difficult to overstate the importance of the 1980 Unfairness Policy Statement in the history of the FTC: Narrowing the scope of unfairness to focus on consumer injury was essential to ensuring the political survival of the FTC as an institution — so damaged was its credibility by its adventur-

---

[61] *See* Commissioner Joshua D. Wright, Proposed Policy Statement Regarding Unfair Methods of Competition under Section 5 of the Federal Trade Commission Act (June 19, 2013), *available at* http://www.ftc.gov/speeches/wright/130619umcpolicystatement.pdf; Commissioner Maureen K. Ohlhausen, Section 5: Principles of Navigation (July 25, 2013), Remarks at the U.S. Chamber of Commerce, *available at* http://ftc.gov/speeches/ohlhausen/130725section5speech.pdf.

[62] *See, e.g.*, FTC Withdraws Agency's Policy Statement on Monetary Remedies in Competition Cases Will Rely on Existing Law (Jul. 31, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies.

[63] *See* Statement of Commissioner Maureen K. Ohlhausen, Dissenting from the Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases (Jul. 31, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120731ohlhausenstatement.pdf.

[64] *See* Magnuson-Moss Warranty-Federal Trade Commission Improvement Act (Lemon Law), Pub. L. No. 93-637, 88 Stat. 2183 (codified at 15 U.S.C. §§ 2301-2312 (2000)); *see also* Beales, *supra* note 4.

ism and boundless legal claims of authority in the 1970s.[65] It's not surprising, then, that Congress in 1994 (a heavily Democratic Congress, as in 1980) codified the UPS into law.[66] Indeed, the 1994 amendment actually narrowed the scope of unfairness even further in a way so subtle it is rarely acknowledged: by clarifying that "public policy considerations may not serve as a primary basis for [determining that a practice is unfair],"[67] something the UPS *had* allowed.

The 1983 Deception Policy Statement was less politically contentious, but in substantive ways no less important. Just as the UPS resolved a heated debate about the need for the FTC to establish *consumer injury*, the DPS resolved a heated debate about the need for the FTC to establish *materiality*.[68] In both cases, the FTC abandoned the position it had taken in the 1970s: that it had free rein to act without evidence of harm or materiality — which, it clarified in the UPS, was simply a proxy for injury.[69] Both Statements also reflected compromises between the FTC's earlier positions and more radical curtailing of the FTC's authority: abolishing unfairness altogether or abolishing the presumption of materiality.

Yet the two Statements differ in one crucial respect: Congress has never codified, let alone curtailed, the DPS. The 1994 codification of the UPS marks not only the last time Congress modified the FTC Act, but also the last time it reauthorized the Commission.[70] This means that, strictly speaking, the Deception Policy Statement isn't actually binding on the FTC the way that a statute or judicial decision is; subject to certain constraints, the FTC can always change its mind.[71]

Back in 1999, in the FTC's very first "information broker" case (*TouchTone*), the Commission found that the "pretexting" company had deceived not consumers but the banks that held their information when its representatives pretended to be the customer in order to gain access to information about the customer.[72] In addition to its unfairness claim, the Commission insisted that the DPS:

> was not issued by this agency to serve as a straitjacket for Section 5's deception authority. This Commission has never so held. And, with due respect to [dissenting Commissioner Swindle's] unduly narrow interpretation, no Court of Appeals has

---

[65] *See* Beales, *supra* note 4.

[66] Codified at 15 U.S.C. §45 (2012).

[67] *Id.* at §45(n).

[68] *See* Deception Policy Statement, *supra* note 6.

[69] *Id.* at 191("Injury exists if consumers would have chosen differently but for the deception. If different choices are likely, the claim is material, and injury is likely as well. Thus, injury and materiality are different names for the same concept.").

[70] The FTC has thus been operating for 21 years — an entire generation — on short-term appropriations, something that is highly unusual even in today's era of a dysfunctional legislative branch.

[71] *See supra* n.51 and accompanying text.

[72] *See* FTC v. TouchTone, Complaint, Civil Action No. 99-WM-783 (D. Colo. 1999), *available at* https://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtonecomplaint.htm.

> found the Statement to preclude challenging as deceptive certain acts or practices that were not foreseen at the time or described within its four corners.[73]

In other words, the FTC refuses to be constrained by its own policy statement. It has brought at least some cases that appear to go beyond the "four corners" of the DPS. A year after *Touch-Tone*, the FTC brought another enforcement action based on business-to-business deception, this time claiming that tech giant eBay was deceived by the upstart Reverse Auction.[74] More recently, the Commission has wielded its deception authority in business-to-business conduct concerning standard-essential patents — over the strong dissent of Commissioner Ohlhausen.[75]

FTC Process Reform Legislation

At a minimum, Congress could pass legislation that looked something roughly like Section 5(n) of the FTC Act:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[76]

Language written at this high conceptual level could help — simply by codifying what the DPS already says. But to actually address the problem illustrated by the *Nomi* settlement, the legislation would likely have to be more granular. Where Congress was able to distill the key provisions of the UPS into one sentence, and narrow it further with another, clarifying the definition of materiality would be harder. It would likely require more clearly defining the *process* by which materiality is defined, including:

Appropriately constraining the FTC's discretion without hamstringing the agency's legitimate consumer protection efforts — creating an administrable rule but not a blank check — would not be easy, just as it was not when the FTC wrote either Policy Statement, either. But Congress could draw on at least three sources of authority to assist it:

1. FTC Commissioners, each of which could be invited to suggest language;

---

[73] In the Matter of Touch Tone Information, Inc., File No. 982-3619, Statement of Chairman Pitofsky & Commissioners Anthony & Thompson, *available at* https://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-majoritystatement.htm.

[74] FTC v. ReverseAuction.com, Inc., Complaint. *available at* http://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm.

[75] *See* In re Robert Bosch GmbH, FTC File No. 121-0081, Statement of Commissioner Maureen K. Ohlhausen, at 3- 4 (Nov. 26, 2012), *available at* http://www.ftc.gov/os/caselist/1210081/121126boschohlhausenstatement.pdf.

[76] 15 U.S.C. § 45(n) (2012).

2. Congress's usual legislative process, including both hearings and a GAO study; and
3. A Privacy Law Modernization Commission, such as we have proposed.[77]

But if the FTC's experience in recent decades has taught us anything, it is that articulating better substantive standards is only half the problem — whether in policy statements (*e.g.,* UPS, DPS) or in binding, statutory form (*e.g.,* Section 5(n)). These constraints will mean little if the FTC is not subject to some external constraint. Clearer standards might spur more statements by Commissioners and thus more analysis of each case, but they will never supplement for the key missing ingredient: litigated decisions by which Article III courts enforce these limiting principles.[78]

Possible specific reforms Congress should consider include:

1. Creating a standard for settling cases that:
    a. Is higher than the very low bar set by Section 5(b) for *bringing* the investigation;
    b. Requires the FTC to clearly tie the consent decree to the conduct at issue (something that, in theory, is required by the Supreme Court's 1968 *Colgate-Palmolive* decision,[79] but which the Commission has consistently failed to do);
2. Requiring that the FTC say more in each settlement about its legal claims;
3. Making settlements subject to judicial review;
4. Vesting one Commissioner with veto power over a settlement: the right to insist that the matter be referred to a federal court, which would decide whether the FTC had satisfied its burden. In the absence of a defendant willing to litigate the matter, that Commissioner could even be given statutory standing to argue the case in court.
5. Re-examining the Commission's Compulsory Investigative Demand (CID) process to ensure that it does not, through its cost and lack of due process, facilitate the FTC coercing settlements based on questionable legal claims;
6. Requiring the FTC to issue retrospective guidelines summarizing the doctrinal trends in its enforcement actions, akin to the FTC and DOJ's various merger guidelines; and
7. Requiring the FTC to publish more guidance on cases it did *not* bring, either in the form of
    a. Closing letters;
    b. Analysis in guidelines; or

---

[77] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), *available at* http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf ("A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.").

[78] *See* Szoka, *supra* note 23.

[79] FTC v. Colgate-Palmolive Co., 380 U.S. 374, 392 (1968) (an order's prohibitions "should be clear and precise in order that they may be understood by those against whom they are directed," and that "[t]he severity of possible penalties prescribed . . . for violations of orders which have become final underlines the necessity for fashioning orders which are, at the outset, sufficiently clear and precise to avoid raising serious questions as to their meaning and application.") (internal citations omitted).

c. Annual reports that summarize such cases without identifying the parties;

This is merely an illustrative list of more obvious examples. Since the FTC's processes have not been substantially modified (or probably even re-examined) by Congress since 1980, and even the 1980 assessment focused on rulemaking, not enforcement, any proper reauthorization of the agency will likely involve many more, smaller changes, including reassessment of processes and organizational structure. FTC Commissioners and staff will play one of three roles in such a process, and in helping bring it about:

1. Ideally, they will be an active, constructive participant, helping Congress understand both sides of each issue, the tradeoffs between administrability and rigor of legal standards, and the error costs of both making the FTC's job too easy and making it too hard — just as in 1982-3, Chairman Miller and other Commissioners presented very different visions of deception (require not just materiality but proof of harm vs. allow the Commission to generally presume materiality), and the Commission reached the middle ground of the DPS whose precise application is at issue in *Nomi*.
2. Conversely, the Commission could simply drag its heels, stonewalling any efforts to constrain the FTC's discretion or provide guidance to those regulated by it — as the current FTC leadership has stonewalled proposals by Commissioners Wright and Ohlhausen for a Policy Statement on Unfair Methods of Competition[80] — and these issues will simply fester indefinitely.
3. Congress may simply have to compel the agency to cooperate against its will, just as Congressional leaders of both parties forced the FTC in 1980 to issue the Unfairness Policy Statement.

Conclusion

Nomi will undoubtedly be remembered as the first in what is sure to be a series of cases dealing with collection of data "offline" — a distinction that will likely increasingly seem quaint as the "Internet" permeates our everyday lives. Its true importance, however, has little to do with the specifics of the case (*e.g.*, in-store signage, creative systems for pushing notification to users about tracking) and everything to do with doctrine and process.

The majority's logic reveals its true conception of deception, one in which the materiality requirement so essential to the Deception Policy Statement is reduced to a mere formality. By refusing to adequately weigh competing evidence, the Commission has claimed maximum discretion — the very opposite of "doctrine," which is best understood as a conceptual framework or procedural steps that the agency is supposed to use to decide particular cases.

What the case says about the FTC's processes may be even more disturbing: yet again, completely outside the legal system, the FTC has made a significant leap in doctrine, nullifying *the* core element of what is supposed to be one of its two foundational Policy Statements. Nomi was not willing to litigate the case, and so the matter stands at its unsatisfying end: In a few sentences, the complaint lays out a theory of deception that is difficult to reconcile with the DPS and is

[80] *See supra* note 61.

supported by less than two pages of legal analysis by the majority. Even that much analysis was provided only because of the dissent of Commissioner Wright, who objected to the majority's legal analysis (not merely its exercise of prosecutorial discretion, as did Commissioner Ohlhausen). If anything, the *Nomi* case is remarkable not for how little legal analysis it contains, but for how *much* it contains relative to the many other cases where the FTC made small leaps without objection. This may resemble the "common law" in that it is case-by-case and that it changes over time, but it lacks the essential feature of the common law: rigorous analysis of fine points of doctrine, to ensure that each leap, however small, is actually justified by the overarching doctrines that the FTC is supposed to be applying, understood in their full context.[81]

If "discretion" is the FTC's goal, "attenuation" is the process by which it has achieved that: without judicial review, each case becomes more attenuated from the starting point. Thus the concept of deception has become more attenuated from consumer injury. Materiality was supposed to marry the two, while giving the FTC a more easily administrable rule, yet the FTC has replaced the easier exercise of establishing materiality with a general presumption of materiality, thus attenuating the result even further from the overall purpose of the agency (preventing consumer injury). The same is true for the various factors that are supposed to justify the presumption, like establishing intent (to justify presuming that an omission is material).

At every level of analysis, the pattern is the same: maximize the FTC's discretion and attenuate the analysis as much as possible from an analysis of consumer welfare. Doing so moves the FTC ever further from the compromise enshrined in the DPS, rooted in the uncontroversial recognition that the FTC may sometimes be mistaken in its assessments, and that its interventions may do consumers more harm than good.

That pattern is unlikely to change unless Congress intervenes to return the FTC to the Deception Policy Statement *and* also to ensure that the courts play a greater role in scrutinizing the agency's leaps in the future. Otherwise, the pattern of maximizing discretion through attenuation will simply play out again and again.

---

[81] *See* Manne & Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law," supra* note 22 at 8 ("The common law thus emerges through the accretion of marginal glosses on general rules, dictated by new circumstances.").

Testimony of

TechFreedom

Berin Szóka[1] & Graham Owens[2]

FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare

Hearing before the Subcommittee on Consumer Protection, Product Safety, Insurance, & Data Security of the U.S. Senate Committee on Commerce, Science, & Transportation

Tuesday, September 26, 2017

2:30 p.m.

Russell Senate Office Building
Room 253

---

[1] Berin Szóka is President of TechFreedom, a nonprofit, *nonpartisan* technology policy think tank. J.D. University of Virginia School of Law; B.A. Duke University. He can be reached at bszoka@techfreedom.org. With thanks to my dedicated legal staff at TechFreedom, and in particular Vinny Sidhu and Sunny Seon Kang.

[2] I. Graham Owens is a Legal Fellow with TechFreedom. J.D. George Washington University School of Law; B.A. University of Virginia. He can be reached at gowens@techfreedom.org.

Table of Contents

I. Introduction

Over the last two decades, use of, and access to, the Internet has grown exponentially, connecting people and businesses and improving the human condition in ways never before imagined. In 2011, 71.7% of households reported accessing the Internet, a sharp increase from 18 percent in 1997 and 54.7% in 2003.[3] This digital growth — from a network of computers that only a few consumers could reach, to a seemingly infinite marketplace of ideas accessible by almost all Americans — has benefited society beyond measure, affording consumers the ability to access information, purchase goods and services, and interact with each other almost instantaneously without having to leave the home.[4]

However, as use and benefits of the Internet has grown, so too has the collection of personal data and, consequently, cyber-attacks endeavoring to steal that data. Since 2013, the number of companies facing data breaches has steadily increased.[5] In 2016, 52% of companies reported experiencing a breach — an increase from 49% in 2015 — with 66% of those who experienced a breach reporting multiple breaches.[6] Perhaps not surprisingly, not much has changed since 2000, where one report revealed that system penetration by outsiders grew by 30% from 1998 to 1999.[7] Interestingly, despite immense improvements in companies' ability to anticipate and prevent cyber-attacks, some of the largest and most sophisticated companies in the world, including Sony, Target, eBay, and JPMorgan, continue to experience data breaches today,[8] just as they did in 2000.[9] In spite of these statistics, the United States currently has no comprehensive legal framework in which to inform companies of the best

---

[3] THOM FILE, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES 1 (May 2013), https://www.census.gov/prod/2013pubs/p20-569.pdf; *see also* Steve Case, The Complete History of the Internet's Boom, Bust, Boom Cycle, Business Insider (Jan. 14, 2011), *available at* http://www.businessinsider.com/what-factors-led-to-the-bursting-of-the-internet-bubble-of-the-late-90s-2011-1.

[4] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 1 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[5] PONEMON INST. LLC, FOURTH ANNUAL STUDY: IS YOUR COMPANY READY FOR A BIG DATA BREACH? 1 (2016), http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-preparedness-study.pdf [hereinafter PONEMON, DATA BREACH].

[6] *Id.*

[7] Hope Hamashige, *Cybercrime can kill venture*, CNN (March 10, 2000), http://cnnfn.cnn.com/2000/03/10/electronic/q_crime/index.htm (reporting the findings of the Computer Security Institute at Carnegie Mellon University).

[8] PONEMON INST. LLC, 2014: A YEAR OF MEGA BREACHES 1 (2015), http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

[9] Hamashige, *Cybercrime* (noting that, just as today, in 2000, "[e]ven the biggest Internet companies with the most sophisticated technology are vulnerable to hackers, a trend highlighted last month when hackers stopped traffic on several popular Internet sites including Yahoo!, Amazon.com and eBay.").

practices to both prevent or respond to cyber-attacks, as well as to ensure that they're acting responsibly in the eyes of the Government.[10]

Absent a comprehensive statutory framework, the Federal Trade Commission ("FTC" or "Commission") happily stepped in to police the vast number of data security and privacy practices not covered by the few Internet privacy and cyber security statutes enacted at the time. For two decades, the FTC has grappled with the consumer protection issues raised by the Digital Revolution. Armed with vast jurisdiction and broad discretion to decide what is unfair and deceptive, the agency has dealt with everything from privacy to data security, from online purchases to child protection, and much more. The FTC has become the Federal *Technology* Commission — a term we coined,[11] but which the FTC and others have embraced.[12]

This was inevitable, given the nature of the FTC's authority. Enforcing the promises made by tech companies to consumers forms a natural baseline for digital consumer protection. On top of that deception power, the FTC has broad power to police other practices, without waiting for Congress to catch up. As the FTC said in its 1980 Unfairness Policy statement:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion.[13]

---

[10] *See, e.g.,* ALAN CHARLES RAUL, TASHA D MANORANJAN & VIVEK MOHAN, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268 (Alan Charles Raul, 1st ed. 2014) ("With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather, allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin, 'unfair or deceptive' business practices.").

[11] Berin Szóka & Geoffrey Manne, The Second Century of the Federal Trade Commission, TECHDIRT (Sept. 26, 2013), available at https://www.techdirt.com/blog/innovation/articles/20130926/16542624670/secondcentury-federal-trade-commission.shtml; see also Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission, Report 1.0 of the FTC: Technology & Reform Project, 3 (Dec. 2013), available at http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[12] Kai Ryssdal, The FTC is Dealing with More High Tech Issues, MARKETPLACE (Mar. 7, 2016) (quoting then-Chairman Edith Ramirez), available at http://www.marketplace.org/2016/03/07/tech/ftc-dealing-more-high-tech-issues.

See, e.g., Omer Tene, *With Ramirez, FTC became the Federal Technology Commission*, IAPP (Jan. 18, 2017), https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/.

[13] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (hereinafter 1980 Unfairness Policy Statement).

The question is not whether the FTC *should* be the Federal Technology Commission, but *how* it wields its powers. For all that academics like to talk about creating a Federal Search Commission[14] or a Federal Robotics Commission,[15] and for all the talk in Washington of passing "comprehensive baseline privacy legislation" or data security legislation, the most important questions turn on the FTC's processes, standards, and institutional structure. How the FTC and Congress handle these seemingly banal matters could be even more important in determining how consumer protection works in 2117 than will any major legislative lurches over the next century. Indeed, with the costs of cybercrimes expected to reach $2 trillion by 2019,[16] the business community can ill afford to have to anticipate the approaches of both hackers and federal regulators simultaneously, and it would seem more practical for the agency to help guide businesses by providing best practices to better protect their consumers. Yet, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which do not admit liability and only focus on prospective requirements of the specific defendant in that case.[17]

This approach, and the resulting ambiguity, has left companies facing uncertainty in terms of whether their data security and privacy practices are not only sufficient to safeguard against an FTC enforcement action, but more importantly, whether they're utilizing the best practices available to protect their consumers' data and privacy.

---

[14] *See, e.g.,* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008), *available at* http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Bracha-Pasquale-Final.pdf.

[15] *See, e.g.,* Ryan Calo, *The case for a federal robotics commission*, Brookings Institute (Sept. 15, 2014), *available at* https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/; Nancy Scola, *Why the U.S. might just need a Federal Commission on Robotics*, Washington Post (Sept. 15, 2014), *available at* https://www.washingtonpost.com/news/the-switch/wp/2014/09/15/why-the-u-s-might-just-need-a-federal-commission-on-robots/?utm_term=.38dfc4bec72e.

[16] Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, Forbes (Jan. 17, 2016), *available at* https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6e10063a3a91.

[17] *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257, n.22. (3d Cir. 2015). Notably, this practice is not entirely limited to data security and privacy enforcement — though for reasons later discussed, the effects on companies are arguably more severe in this context — by the Commission, with one study finding that 1,524 of the 2,092 enforcement action brought by the FTC in either federal or administrative courts have ended in consent decrees without any adjudication. This means that almost 73% of the FTC's enforcement actions have ended in legally enforceable orders, despite no impartial judicial guidance as to the factual and legal legitimacy of the FTC's claims. *See* Daniel A. Crane, *Debunking Humphrey's Executor*, 83 GEO. WASH. L. REV. 1835, 1867 (2015). But in tech-related cases its almost 100%, meaning the courts have played essentially no role at all in disciplining the FTC's use of unfairness in "informational injury" cases. *See infra* note 122 (providing list of a few cases that did not result in settlement).

Understandably, this ambiguity has frustrated judges and legal commentators alike, even resulting in one company's demise. Such frustration was made abundantly clear by the Third Circuit when, despite affirming the FTC's authority to regulate cyber security practices under the "unfair practices" prong of Section 5, the court nonetheless questioned the Commission's assertion that its consent decrees and "guidance" somehow create standards against which companies' cyber practices can be tested for "unfairness."[18] In fact, the Third Circuit emphatically agreed with the defendant's claim that "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a)."[19] The court continued:

> We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." Oral Arg. Tr. at 51. We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples. *Id.* at 52.[20]

The court's frustration did not end with the Commission's use of consent decrees either, making sure to also address issues with the FTC's 2007 guidebook, *Protecting Personal Information, A Guide for Businesses*, which, according the FCC, "describes a 'checklist[]' of practices that form a 'sound data security plan.'"[21] Ultimately, the court recognized that "[t]he guidebook does not state that any particular practice is required by [Section 5]," and "[f]or this reason, we agree … that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[22]

Despite being rebuked by practitioners and courts alike, the FTC has brushed aside this frustration and continued to rely on consent decrees, conclusory guidebooks/reports, and "blog posts" to inform businesses as to what constitutes reasonable data security and privacy practices. By contrast, the FTC has pursued a radically different course, providing significantly more thorough guidance in an area not considered to be the FTC's primary jurisdiction — environmental regulations through "Green Guides." As explained below, these Green Guides

---

[18] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 252-253, 255 (3d Cir. 2015).

[19] *Id.* at 257 n.22.

[20] *Id.* at 257 n.23.

[21] *Id.* at 257.

[22] *Id.* at 257 n.21.

reflect a sincere and thoughtful effort by the FTC to gather relevant data as the basis for analyzing not only "what" is required, but more significantly "why" is it essential and "how much" of a certain practice is necessary.

On privacy and data security, the Commission has refused to do such empirical work or to issue clear guidance, relying instead on consent decrees and conclusory reports and guidebooks that lack any evident empirical foundation. This has deprived businesses of the regulatory certainty and clarity they need to comply with the law — and deprived consumers of better, more consistent data security and privacy practices. The Commission has flaunted the warning given it by the D.C. Circuit over forty years ago, that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible.[23] Ironically, the D.C. Circuit made that statement in a case where the FTC fought vehemently — and the court agreed — for the authority to provide the very guidance they refuse to provide to the digital economy today. Congress *did* provide that rulemaking authority a year later, with the Magnuson-Moss Act of 1975,[24] but also found it necessary to institute new procedural safeguards in 1980, after the FTC's gross abuse of its rulemaking powers in the intervening five years,[25] which culminated in the agency being denounced as the "National Nanny."[26]

With this backdrop in mind, I come before this Committee today with two goals. First, to inform this body — through a historical lens — of the FTC's ongoing procedural issues, particularly as they pertain to data security and privacy practices. Second, to use that historical analysis as a framework with which to propose practical process reforms that will ensure American businesses and the FTC work together as partners, not enemies, to make certain that consumers'—including Americans as well as foreign consumers who patronize U.S. businesses—data and privacy are afforded the greatest respect and protection possible.

---

[23] *Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974).

[24] The Magnuson-Moss Warranty Federal Trade Commission Improvement (Magnuson-Moss) Act, Pub.L.No. 93-637, § 202(a), 88 Stat. 2193 (1975).

[25] The Federal Trade Commission Improvements Act of 1980 (Improvements Act), Pub.L. No. 96-252, 94 Stat. 374 (1980).

[26] Editorial, WASH. POST (Mar. 1, 1978), reprinted in MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION, 69–70 (1982); *see also* J. Howard Beales III, *Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present*, 8 n.37 (2004), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kidsand-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf. ("Former FTC Chairman Pertschuk characterizes the Post editorial as a turning point in the Federal Trade Commission's fortunes.").

To that end, we herein provide a more in-depth historical analysis of the FTC's enforcement authority, including an examination of the problems that have arisen due to the FTC's current procedural issues. We detail how the FTC has utilized data-driven guidance in other contexts — namely the aforementioned Green Guides — to guide businesses through empirical analysis of available data. Finally, we use that historical context to frame ways that Congress can help urge the FTC to provide the same types of empirical guidance to the tech industry. Finally, I will discuss the underlying issues with the FTC's *very* low pleading standard and examine ways that Congress can address this problem.

Background of FTC Enforcement in the Digital Economy

While the FTC began studying online privacy issues as early as 1995,[27] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[28] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[29] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[30] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[31] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought

---

[27] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (June 1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter 1998 FTC Privacy Report] ("In April 1995, staff held its first public workshop on Privacy on the Internet, and in November of that year, the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues."); *see also* FED. TRADE COMM'N, A REPORT FROM THE FEDERAL TRADE COMMISSION STAFF: THE FTC'S FIRST FIVE YEARS PROTECTING CONSUMERS ONLINE (Dec. 1999), *available at* https://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-online/fiveyearreport.pdf.

[28] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[29] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[30] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[31] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[32] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[33] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[34] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[35]

In a speech last week, Acting Chairman Ohlhausen broadly summarized the "various types of consumer injury addressed in our privacy and data security cases" as "informational injury."[36] It's a useful shorthand: one term to describe a cluster of consumer protection problems behind a wide range of cases. But for the same reason, it's also a dangerous term — one that could, like "net neutrality," take on a life its own, and serve to obscure and frustrate analysis rather than inform it.[37] Of course, Chairman Ohlhausen chose her words carefully:

> [L]et me also emphasize that this is not a discussion of the legal question of what constitutes a 'substantial injury' under our unfairness standard. My topic today

---

[32] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[33] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[34] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[35] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[36] Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Painting the Privacy Landscape: Information Injury in FTC Privacy and Data Security Cases, Address Before the Federal Communications Bar Association (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf [hereinafter Ohlhausen, *Informational Injury Speech*].

[37] Larry Downes, *The Tangled Web of Net Neutrality and Regulation*, Harvard Business Review (March 31, 2017), *available at* https://hbr.org/2017/03/the-tangled-web-of-net-neutrality-and-regulation ("Despite being a simple idea, net neutrality has proven difficult to translate into U.S. policy. It sits uncomfortably at the intersection of highly technical internet architecture and equally complex principles of administrative law. Even the term "net neutrality" was coined not by an engineer but by a legal academic, in 2003."). Gerard Stegmaier, a veteran attorney in the field of data security and privacy, explained it as such: "Words matter. Net Neutrality. Deep Packet Inspection. #Privacy. Businesses beware. There's a new label in town from the gov't and repeating it could have significant unintended consequences. From a speech yesterday the @FTC acting chair declared "informational injuries" exist. Let that sink in." Posting of Gerard Stegmaier on LinkedIn.com (Sept. 20, 2017), *available at* https://www.linkedin.com/feed/update/urn:li:activity:6316291846356115456 (also on file with author).

> may inform the substantial injury question, but I am speaking more broadly. Indeed, many of the cases I will mention are deception cases, or allege both deception and unfairness.
>
> …
>
> In my review of our privacy and data security cases, I have identified at least five different types of consumer informational injury. Certain of these types are more common. Many of our cases involve multiple types of injury. Courts and FTC cases often emphasize *measurable* injuries from privacy and data security incidents, although other injuries may be present. And to be clear, not all of these types of injury, standing alone, would be sufficient to trigger liability under the FTC Act. [38]

It is fitting that she should emphasize the word "measurable" — and also caveat it with the word "often" — because both speak to the central question facing the Federal Technology Commission as it grapples with an endless, and accelerating, parade of novel consumer protection issues: *how* does the agency determine what the right answer is in any particular case and what should be done about it? Ohlhausen defended the FTC's approach to privacy and data security enforcement:

> Case-by-case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. As such, each case integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury.[39]

Yes, the courts' "feedback" is "important." Indeed, in a reply brief the FTC expressly agreed with TechFreedom on this importance of courts' guidance when it said it "agrees that the field would be aided by a body of law that includes 'Article III court decisions.'"[40] Yet, such assertions of the importance of courts' "feedback" by the FTC seem empty given there has been precious little of it. Since 1997, not counting a handful of cases where the FTC sought

[38] Ohlhausen, *Informational Injury Speech*, *supra* note 36, at 2-3.

[39] Ohlhausen, Informational Injury Speech, supra note 36, at 2.

[40] Plaintiff's Response In Opposition to the Motion to Dismiss, F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015) (No. 2:13-CV-01887-ES-SCM) at 22, n. 8.

injunctive relief against absent defendants (generally foreign scammers), the FTC has litigated, even partially, only a handful of cases: *LabMD*,[41] *Wyndham Worldwide Corp.*,[42] *Amazon.com, Inc.*,[43] and *D-Link Systems, Inc.*[44] Thus, the way the FTC works today is a far cry from what the FTC said about how it would operate back in 1980:

> The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[45]

What former FTC Chairman Tim Muris said of the Commission in 1981 remains true today: "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[46] As he noted in his 2010 testimony before a Senate Subcommittee, "the Commission's authority remains extremely broad."[47] What Commissioner Wright said of the FTC's competition enforcement — where the Commission differs from the DOJ in enforcing (in theory, anyway) the same substantive laws — is even more true of consumer protection:

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may

---

[41] LabMD, Inc. v. F.T.C., No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015).

[42] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[43] *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[44] *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017).

[45] 1980 Unfairness Policy Statement, *supra* note 12 (quoting *FTC v. Raladam Co.*, 283 U.S. 643, 648 (1931)).

[46] Timothy J. Muris, Judicial Constraints, in THE FEDERAL TRADE COMMISSION SINCE 1970: ECONOMIC REGULATION AND BUREAUCRATIC BEHAVIOR, 35, 49 (Kenneth W. Clarkson & Timothy J. Muris, eds., 1981).

[47] *Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. 2 (2010) (statement of Timothy J. Muris, Former Chairman, Fed. Trade Comm'n) *available at* http://lawprofessors.typepad.com/files/muris_senate_testimony_ftc_role_protecting_consumers_3-17- 101.pdf.

> not [violate any law or regulation]. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's [Section 5] authority by encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority.[48]

Without the courts to demand rigor from the FTC in defining "measurable" harm, what should the Commission do? And what should Congress do?

Chairman Ohlhausen's speech represents a major step in the right direction — precisely because it promises to give more analytical rigor to the term "informational injury" than such generalizations generally have. She concludes:

> This analysis raises several important questions. Is this list of injuries representative? When do these or other informational injuries require government intervention? Perhaps most importantly, how does this list map to our statutory deception and unfairness authorities?
>
> These are critical and challenging questions. That's why I am announcing today that the FTC will host a workshop on informational injury on December 12 of this year. This workshop will bring stakeholders together to discuss these issues in depth. I have three goals for this workshop: First, better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents. Second, explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence. And third, better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information. Ultimately, the goal is to inform our case selection and enforcement choices going forward.[49]

Amen. This is the kind of workshop the FTC should have held two decades ago — and several more times since. The FTC has, in fact, conducted such workshops, collected empirical data,

---

[48] Joshua D. Wright, *Revisiting Antitrust Institutions: The Case for Guidelines to Recalibrate the Federal Trade Commission's Section 5 Unfair Methods of Competition Authority*, 4 CONCURRENCES: COMPETITION L.J. 1 at 3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/siting-antitrust-institutions-case-guidelines-recalibrate-federal-trade-commissions-section-5-unfair/concurrences-4-2013.pdf.

[49] Ohlhausen, *Informational Injury Speech*, *supra* note 36 , at 9.

and issued corresponding guidance based upon rigorous empirical analysis in another context: the Green Guides first issued for environmental marketing in 1992, and updated three times since then.[50] As discussed below, these offer an excellent model for how the Commission could begin to take a more substantive approach to defining informational injury, while also providing clearer guidance to industry.

Congress should support and encourage this effort — by holding the FTC to the high standards set by its work on the Green Guides. If this effort represents a significant departure with the analytically flimsy, "know-it-when-we-see-it" approach the FTC has generally taken to "informational injury" cases thus far, both consumers and companies would benefit from clearer, better substantiated guidance. But this will not be an easy change to make; it will require a new degree of rigor in how the Bureau of Consumer Protection operates, and a new closeness in BCP's engagement with the Bureau of Economics.

At best, this could be the beginnings of a "law and economics" revolution in consumer protection law — of the sort that transformed competition law in decades past, has guided the Bureau of Competition since, and has informed the courts in their development of antitrust case law.

But at worst, this process could result in blessing the FTC's current approach with a veneer of analytical rigor that merely validates the status quo. The report that comes out of this process *could* resemble the reports the FTC has produced since the 2012 Privacy Report, which make broad recommendations as to what industry best practices should be, without any real analysis behind those recommendations or how they relate to the Commission's powers under Section 5.[51]

Chairman Ohlhausen's initial thoughtful framing suggests reason for optimism, but everything will depend on how she and whoever becomes permanent Chairman (if it is not her) execute on the plan. In any event, the Commission's own more recent experience with the

---

[50] *See* Fed. Trade Comm'n, *Environmental Friendly Products: FTC's Green Guides* (last visited Sept. 24, 2017), available at https://www.ftc.gov/news-events/media-resources/truth-advertising/green-guides ("The Green Guides were first issued in 1992 and were revised in 1996, 1998, and 2012. The guidance they provide includes: 1) general principles that apply to all environmental marketing claims; 2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and 3) how marketers can qualify their claims to avoid deceiving consumers.").

[51] *See* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE 57-60 (2016), *available at* http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf [hereinafter White Paper].

Green Guides — to say nothing of the last 15 years of experience with data security and privacy — suggests that self-restraint is unlikely to prove sustainable, on its own, in disciplining the agency. Ultimately, the kind of analytical quality that has defined antitrust law, and has sustained the law and economics approach there, requires *external* constraints — namely, regular engagement with the courts and oversight by Congress.

To that end, a careful reassessment of the Commission's processes is long overdue. The last time Congress seriously reconsidered, and revised, the FTC's processes was in 1994.[52] The agency has not been reauthorized since 1996.[53] Congress should return to its habit — the default assumption prior to Ken Starr, Monica Lewinsky, and impeachment — of reauthorizing the FTC every two years and, each time, re-examining how well the agency is working. Modifications to the statute should not be made lightly, but they should also happen more often than once in a generation.

Last year, the House Committee on Energy and Commerce considered no fewer than seventeen bills regarding the FTC. The attached white paper, co-authored with Geoffrey Manne, Executive Director of the International Center for Law & Economics, surveys those bills and provides recommendations to Congress on how to approach them.[54] Together, they form a starting point for the Senate Commerce Committee to begin its work, but they do not cover many of the most important aspects of how the agency works. Given this Committee's extensive knowledge and expertise, we hope that this Committee, along with the broader Senate, should start its own work on FTC reform legislation afresh.

II. Summary of Proposed Legislative Reforms

Rather than repeat the full analysis provided in the aforementioned white paper we presented to the House Energy & Commerce Committee last year, we have instead provided a short overview of how to consider thinking about the main issues we believe need to be addressed through legislation.

---

[52] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691 (Aug. 26, 1994) *available at* http://uscode.house.gov/statutes/pl/103/312.pdf.

[53] Federal Trade Commission Reauthorization Act of 1996, Pub. L. 104-216, 110 Stat. 3019 (Oct. 1, 1996), *available at* http://uscode.house.gov/statutes/pl/104/216.pdf.

[54] *See generally* White Paper, *supra* note 51.

A. The Common Carrier Exception

The FTC Act excludes "common carriers subject to the Acts to regulate commerce."[55] What this provision means will be crucial — especially for technology cases in the coming years — and merits clarification from Congress.

The Federal Communications Commission has proposed to undo its 2015 reclassification of broadband providers as common carriers.[56] Doing so will return the controversial issue of "net neutrality" to the Federal Trade Commission by restoring the FTC's jurisdiction over broadband providers — or rather, there *should* be a seamless transition to ensure that consumers remain protected. But a Ninth Circuit panel decision last year calls into question whether the FTC's jurisdiction will be fully restored,[57] creating the possibility that a company providing broadband service, once that service is no longer considered a common carrier service by the FCC, might still remain outside the jurisdiction of the FTC either because (1) that particular corporate entity also provides a common carrier service such as voice (which will remain subject to Title II of the Communications Act even after the FCC's proposes re-reclassification of broadband) or (2) another corporate entity under common ownership provides such a common carrier service. In short, the panel decision rejected the FTC's longstanding "activity-based" interpretation of the statute in favor of an "entity-based" interpretation. The Ninth Circuit granted rehearing of that decision earlier this year, effectively vacating the panel decision.[58]

At oral arguments last week, AT&T stuck by its general arguments for an entity-bases interpretation, but clarified two things.[59] First, it read the statute to turn on the common carrier or non-common carrier status of each specific corporate entity, so that the FTC's jurisdiction over Oath, for example, the company formed by the Verizon parent company after it acquired AOL and Yahoo! and merged them together, would not be affected by the fact that Verizon Wireless provides a common carrier voice service. Second, AT&T argued that the FCC has plenary jurisdiction to, as it did in the *Computer Inquiries*, mandate such structural separation to ensure that there is no gap in consumer protection between the FTC and FCC.[60]

---

[55] 15 U.S.C. § 45(a).

[56] Notice of Proposed Rulemaking, Restoring Internet Freedom, WC Docket No. 17-108, 32 FCC Rcd 4434 (2017), https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1_Rcd.pdf.

[57] *Fed. Trade Comm'n v. AT & T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), *reh'g en banc granted sub nom*., *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017).

[58] Fed. Trade Comm'n v. AT&T Mobility LLC, 864 F.3d 995 (9th Cir. 2017).

[59] United States Court of Appeals for the Ninth Circuit, *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (2017), Oral Arguments, *available at* https://www.youtube.com/watch?v=Rs8EQU-KIEw.

[60] *Id.* at 13:50.

It is impossible to predict how the Ninth Circuit might resolve this case, but it is safe to say that if the FCC issues its Third Open Internet Order this year, or even early next year, that decision might well come out before the Ninth Circuit's decision.

Congress should not assume that the Ninth Circuit will fully restore the FTC's activity-based interpretation of its jurisdiction, even though appears to be the most likely result of the case. Congress should, instead, consider quickly moving legislation that would codify that interpretation. Even if the Ninth Circuit en banc panel accepts AT&T's argument and simply narrows the panel decision, that would only solve part of the problem raised by the panel decision. Requiring structural separation between "edge" companies like Oath and broadband companies like Verizon *might* make business sense anyway, but it might not — especially given the ongoing push to restrict the sharing of consumer data *even among corporate affiliates under common ownership*. Furthermore, AT&T's argument would still raise serious questions about which agency will deal with net neutrality and other consumer protection concerns about broadband services once they are returned to Title I: it is difficult to see how the common carrier services provided by these companies, if only telephony, could be functionally separated from the broadband service. Would consumers have to deal with, and subscribe to, two separate services, each offered by a separate corporate entity?

The Ninth Circuit may, of course, reject AT&T's arguments completely, fully reverse the panel decision, and restore the FTC's activity-based interpretation completely. But it would be far better for Congress to resolve this question before the FCC revises the regulatory classification of broadband. It could do so in a one-sentence bill.

Of course, many have argued that the common carrier exception should be abolished, and the Protecting Consumers in Commerce Act of 2016 (H.R. 5239) would have done just that.[61] Simply restoring the activity-based exemption need not be permanent; it could be stop-gap measure that allows Congress time to consider whether to maintain the exemption.

B. More Economic Analysis

As many commentators have noted, the FTC has frequently failed to employ sufficient economic analysis in both its enforcement work and policymaking. Former Commissioner Josh Wright summarized the problem pointedly in a speech entitled "The FTC and Privacy Regulation: The Missing Role of Economics," explaining:

> An economic approach to privacy regulation is guided by the tradeoff between the consumer welfare benefits of these new and enhanced products and services

[61] Protecting Consumers in Commerce Act of 2016, H.R. 5239, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/5239/text.

> against the potential harm to consumers, both of which arise from the same free flow and exchange of data. Unfortunately, government regulators have instead been slow, and at times outright reluctant, to embrace the flow of data. What I saw during my time at the FTC is what appears to be a generalized apprehension about the collection and use of data – whether or not the data is actually personally identifiable or sensitive – along with a corresponding, and arguably crippling, fear about the possible misuse of such data.[62]

As Wright further noted, such an approach would take into account the risk of abuses that will cause consumer harm, weighed with as much precision as possible. Failing to do so can lead to significant problems, including creating disincentives for companies to innovate and create benefits for consumers.

Specifically, Congress or the FTC should require the Bureau of Economics to have a role in commenting on consent decrees[63] and proposed rulemaking,[64] and a greater role in the CID process. But the most effective ways to engage economists in the FTC's decisionmaking would be to raise the FTC's pleading standards and make reforms to the CID process designed to make litigation more likely: in both cases, the FTC will have to engage its economists more closely, either in order to ensure that its complaints are well-plead or to prevail on the merits in federal court.

C. Clarification of the FTC's Substantive Standards

The FTC has departed in significant ways from both the letter and spirit of the 1980 Unfairness Policy Statement and the 1983 Deception Policy Statement. This is mainly due to the FTC essentially having complete, unchecked, discretion to interpret these policy statements as it sees fit — including the discretion to change course regularly without notice. The courts simply have not had the opportunity to effectively implement Section 5(n), nor has the FTC ever really chosen to constrain its own discretion in meaningful ways (as it has done with the Green Guides). Making substantive clarifications to Section 5 will not be adequate without *process* reforms to ensure that these clarifications are given effect over time. But that does not mean they would be without value.

---

[62] Remarks of Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, George Mason University Law and Economics Center (Nov. 12, 2015), *available at* http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

[63] *See* White Paper, *supra* note 51, at 42-43.

[64] *See id*. at 98-100.

In order to clarify the FTC's substantive standards under Section 5, we would suggest the following key changes:

1. Codifying other key aspects of the 1980 Unfairness Policy Statement into Section 5 that were not already added by the addition of Section 5(n) in 1994;
2. Codifying the Deception Policy Statement, just as Congress codified the Unfairness Policy Statement in a new Section 5(n).[65] This issue is explored in greater depth in my 2015 joint comments with Geoffrey Manne on the FTC's settlement of its enforcement action with Nomi Technologies, Inc.[66] Specifically, in codifying the Deception Policy Statement, Congress should:
    a. Clarify — or require the FTC to propose clarifications of — when and how the FTC must establish the materiality of statements about products: it made sense to presume that all express statements were material in the context of traditional advertising: because each such statement was calculated to persuade users to buy a product. But the same cannot *necessarily* be said of the myriad other ways that companies communicate with users today, such as through online help pages or privacy policies (which companies are required to post online, if only by California law).
    b. Require the FTC to meet the requirements of Section 5(n) when bringing enforcement actions based on the "reasonableness" of a company's practices, such as data security.[67]
3. Codify the FTC's 2015 Unfair Methods of Competition Policy Statement, with one small modification: the FTC should be barred from going beyond antitrust doctrine.[68]

[65] *See* White Paper, *supra* note 51, at 21-28.

[66] *In the Matter of Nomi Technologies, Inc.*, Comments of the International Center for Law & Economics & TechFreedom, File No. 1323251 (May 26, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/05/00011-96185.pdf.

[67] *See infra* 69.

[68] *See* White Paper, *supra* note 51, at 28-30; Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

D. Clarifying the FTC's Pleading Standards

Several courts have already concluded that the FTC's deception enforcement actions must satisfy the heightened pleading standards of Section 9(b) of the Federal Rules of Civil Procedure, which applies to claims filed in federal court that "sound in fraud."[69] As explained below, this requirement would not be difficult for the FTC to meet, since the agency has broad Civil Investigative powers that are not available to normal plaintiffs before filing a complaint.[70] There is no reason the FTC should not have to plead its deception claims with specificity.

The same can be said for unfairness claims, even though they do not "sound in fraud." In both cases, getting the FTC to file more particularized complaints is critical, given that the FTC's complaint is, in essentially all cases, the FTC's last word on the matter, supplemented by little more than a press release, and an aid for public comment.

Indeed, the bar should likely be *higher*, not lower for unfairness cases. The attached white paper recommends a preponderance of objective standard for unfairness cases.[71] The critical thing to note is that there is no statutory standard for settling FTC enforcement actions — so the standard by which the FTC really operates is the very low bar set by Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[72] In addition to the substantive clarifications to the FTC's substantive standards, Congress must clarify either the settlement standard or the pleading standard, if not both.

E. Encouraging More Litigation to Engage the Courts in the Development of Section 5 Doctrine and Provide More Authoritative Guidance

Litigation is important for two reasons. First, having to prove its case before a neutral tribunal forces analytical rigor upon the FTC and thus forces it to make better, more informed decisions. Second, court decisions will provide guidance to regulated companies on how to comply with the law that is necessarily more authoritative (since the FTC cannot simply overrule a court decision the way it can change its mind about its own enforcement actions

---

[69] Rombach v. Chang, 355 F.3d 164, 170 (2d Cir. 2004) ("In deciding this issue, several circuits have distinguished between allegations of fraud and allegations of negligence, applying Rule 9(b) only to claims pleaded under Section 11 and Section 12(a)(2) that sound in fraud.").

[70] *See infra* at 19.

[71] *See* White Paper, *supra* note 51, at 18-21.

[72] 15 U.S.C. § 45(b).

or guidance) and also likely (but not necessarily) more detailed and better grounded in the FTC's doctrines.

One major reason companies settle so often across the board is that the FTC staff has the discretion to force companies to endure the process of litigating through the FTC's own administrative process, first before an administrative law judge and then before the Commission itself, before ever having the opportunity to go before an independent, neutral tribunal. The attached white paper explore three options:[73]

1. "[E]mpower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective."[74]
2. Abolish Part III completely, as former Commissioner Calvani has proposed.[75]
3. Require the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery.[76] Requiring the FTC to litigate all cases in federal court (as the SMARTER Act would do for competition cases[77]) might, in principle, prove problematic for the Bureau of Consumer Protection, which handles many smaller cases. Retaining Part III but allowing Commissioners to object to its use might strike the best balance.

F. The Civil Investigative Demand Process

There are many reasons why companies do not litigate privacy and data security cases. Some of them are beyond the control of FTC or Congress — for example, the extreme sensitivity of these issues for companies. Studies by the Ponemon Institute found that "[d]ata breaches are more concerning than product recalls and lawsuits,"[78] with a company's stock price falling

[73] *See* White Paper, *supra* note 51, at 82-85.

[74] *Id.*

[75] *See id*. at 84-85.

[76] *Id.*

[77] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015).

[78] PONEMON, DATA BREACH, *supra* note 5, at 6.

an average of 5% after a data breach is disclosed.[79] Witness the 30% hit Equifax took to its stock price upon revelation of its data breach.[80] Perhaps most illustrative of the sensitivity of these issues was the case of LabMD — a medical testing company and one of the handful of companies who dared litigate against the FTC — which ultimately went out of business due to litigation costs and reputational damage, even though the judge ultimately found that no consumer was injured.[81] But a very significant, if not the biggest, reason why companies reflexively, almost invariably settle their cases is that the process of the FTC's investigation can be punishment enough to make settlement seem more attractive. After enduring a burdensome investigative process, companies (especially start-ups) frequently lack additional resources to defend themselves and face an informational asymmetry given the intrusiveness inherent in the FTC's current process. Even Chris Hoofnagle, who has long advocated that the FTC be far more aggressive on privacy and data security, warns, in his new treatise on privacy regulation at the agency, that

> [T]he FTC's investigatory power is very broad and is akin to an inquisitorial body. On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[82]

This onerous the process inevitably leads to more false-positives as FTC staff becomes invested in fishing expeditions and force such consent decrees regardless of the actual harms on consumers.[83] Other systemic costs of this process include increased discovery burdens on (even blameless) potential defendants, inefficiently large compliance expenditures throughout the economy, under experimentation and innovation by firms, doctrinally questionable consent orders, and a relative scarcity of judicial review of Commission enforcement decisions. Ultimately, this phenomena distorts the FTC's consumer protection mission because the agency can self-select cases that are likely to settle and further its policy goals,

---

[79] *See* Help Net Security, *After a data breach is disclosed, stock prices fall an average of 5%* (May 16, 2017), https://www.helpnetsecurity.com/2017/05/16/data-breach-stock-price/ (detailing a study by Ponemon).

[80] Paul R. La Monica, *After Equifax apologizes, stock falls another 15%* (Sept. 13, 2017), *available at* http://money.cnn.com/2017/09/13/investing/equifax-stock-mark-warner-ftc-probe/index.html.

[81] *See, e.g.,* Cheryl Conner, *When The Government Closes Your Business*, Forbes (Feb. 1, 2014), https://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/#6e7c78971435; Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, Bloomberg (April 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/ ("The one company that didn't settle with the FTC is LabMD. Daugherty hoped, at first, that if he were as cooperative as possible, the FTC would go away. He now calls that phase 'the stupid zone.'").

[82] Darren Bush, The Incentive and Ability of the Federal Trade Commission to Investigate Real Estate Markets: An Exercise in Political Economy, 20-21, available at http://www.antitrustinstitute.org/files/517c.pdf.

[83] *See* Geoffrey A. Manne, R. Ben Sperry & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1 (2015).

rather than choosing cases on the basis of stopping the most nefarious actors and truly protecting consumers. As even former FTC Commissioner Joshua Wright noted, such self-serving personal and agency goals may push agencies to pursue cases "with the best prospect for settlement, cases that will consume few investigative resources, settle quickly, and are more likely to result in a consent decree that provides a continuing role for the agency."[84] Thus, more than any other aspect of the FTC Act or the FTC's operations, it is here that reinvigorated congressional oversight is needed.

The attached white paper explores this topic in great depth. Specifically, we recommend:

1. Reporting on how the agency uses CIDs[85]
2. Making CIDs confidential by default and allowing companies to move to quash them confidentially.[86] Today, fighting an FTC subpoena means the FTC can make the fight public, which may have serious consequences for a company's brand and stock price.
3. Requiring a greater role for Commissioners and economists in supervising the discovery process.[87]

Ultimately, any examination of the FTC's processes should start with arguably the most sacred principle in the American judicial system: innocent until proven guilty. As the Supreme Court made clear in 1895, "[t]he principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law."[88] While it is inarguably true that these cases are very clearly not criminal, it is also true that these companies and their employees face the threat of losing their "life, liberty, and property" as a result of these actions, as evidenced by LabMD. Despite the Administrative Law Judge finding that "the evidence fails to show any computer hack for purpose of committing identity fraud," the employees of LabMD were nonetheless left without employment simply due to "speculation" by the FTC — a word that appeared seventeen times in the ALJ's decision.[89]

Given the sensitive nature of both the type of information involved in these cases, including financial and health information, as well as consumers' sensitivity to reports that their data

---

[84] D.H. Ginsburg & J.D. Wright, *Antitrust Settlements: The Culture of Consent, in* I. William E. Kovacic: An Antitrust Tribute – Liber Amicorum (Charbit et al. eds., February 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/antitrust-settlements-culture-consent/130228antitruststlmt.pdf.

[85] *See* White Paper, *supra* note 51, at 37-40.

[86] *Id.* at 46-48.

[87] *Id.* at 48-53.

[88] *Coffin v. United States*, 156 U.S. 432, 453 (1895).

[89] LabMD, Inc., No. 9357, 2015 WL 7575033, at *48 (MSNET Nov. 13, 2015), https://causeofaction.org/wp-content/uploads/2015/11/Docket-9357-LabMD-Initial-Decison-electronic-version-pursuant-to-FTC-Rule-3-51c21.pdf.

may be in jeopardy, it is of the utmost importance that Congress ensure that innocent businesses' reputations aren't irreparably damaged simply due to "speculation." To be clear: this is not to say that parties who are guilty of implementing nefarious practices should be protected from the court of public opinion. Indeed, as former Commissioner Wright alluded to, implementing processes that would, at the very least, require the FTC to plead its claims with specificity — and, ideally, subsequently prove it on the basis of data-driven standards — prior to dragging a companies' name through the mud would actually ensure the FTC was using its limited resources to *only* go after the worst actors, rather than merely those most likely to settle.

Requiring the FTC to first make a showing beyond "speculation" of harm it alleges before invoking its immensely broad investigatory power, would at least provide businesses and its employees with some level of protection before being labeled as having unsecure data practices and being forced to face the repercussions that inevitably come with such a label. In doing so, Congress would ensure one of the oldest maxims of law in democratic civilizations continues. As Roman Emperor Julian eloquently quipped in response to his fiercest adversary's statement that "Oh, illustrious Caesar! if it is sufficient to deny, what hereafter will become of the guilty?": "If it suffices to accuse, what will become of the innocent?"[90]

G. Fencing-In Relief

The FTC has broad powers under Section 13(b) to include in consent decrees extraordinarily broad behavioral requirements that "fence in" the company in the future.[91] The courts have been exceedingly deferential to the FTC in applying these requirements, though at least one circuit court has rebuked the FTC's broad approach, as explained in the attached white paper.[92] Rather than attempting to limit how the FTC uses its 13(b) powers, Congress should focus on when Section 13(b) applies. As Howard Beales, former director of the Bureau of Consumer Protection, has argued, regarding deception:

> the Commission's use of Section 13(b) remedies should be reevaluated in light of the law's original purpose: [O]ne class of cases clearly improper for awarding redress under Section 13(b): traditional substantiation cases, which typically involve established businesses selling products with substantial value beyond the

[90] *Coffin v. United States*, 156 U.S. 432, 455 (1895).

[91] *See*, *e.g., Kraft, Inc. v. F.T.C.*, 970 F.2d 311, 326 (7th Cir. 1992) ("The F.T.C. has discretion to issue multi-product orders, so called 'fencing-in' orders, that extend beyond violations of the Act to prevent violators from engaging in similar deceptive practices in the future.") (citing *F.T.C. v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

[92] *See* White Paper, *supra* note 51, at 73-75.

> claims at issue and disputes over scientific details with well-regarded experts on both sides of the issue. In such cases, the defendant would not have known ex ante that its conduct was "dishonest or fraudulent." Limiting the availability of consumer redress under Section 13(b) to cases consistent with the Section 19 standard strikes the balance Congress thought necessary and ensures that the FTC's actions benefit those that it is their mission to protect: the general public.[93]

The same logic goes for the kind of unfairness cases the FTC is bringing against high-tech companies, as Josh Wright noted in his dissent in the *Apple* product design case:

> The economic consequences of the allegedly unfair act or practice in this case — a product design decision that benefits some consumers and harms others — also differ significantly from those in the Commission's previous unfairness cases. The Commission commonly brings unfairness cases alleging failure to obtain express informed consent. These cases invariably involve conduct where the defendant has intentionally obscured the fact that consumers would be billed. Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud — the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items. Under this scenario, the allegedly unfair act or practice injures consumers and does not provide economic value to consumers or competition. In such cases, the requirement to provide adequate disclosure itself does not cause significant harmful effects and can be satisfied at low cost. However, the particular facts of this case differ in several respects from the above scenario.[94]

The key point, as Wright argued, is that the Commission is increasingly using unfairness not to punish obviously bad actors or to proscribe conduct that merits *per se* illegality because it is inherently bad, but rather, conduct that presents difficult tradeoffs: How long should consumers remained logged in to an apps store to balance the convenience of the vast majority of users with the possibility that some users with children may find that their children make unauthorized purchases on the device immediately after the parent has logged in? How much, and what kind of, data security is "reasonable?" And so on. These reflect business decisions that are inevitable in the modern economy. The Commission might well be justified in declaring that a company has struck the wrong balance, but it should not treat them exactly as it would obvious fraudsters, who set out to defraud consumers.

---

[93] J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(b) of the FTC Act*, 79 ANTITRUST L. J. 1, 6-7 (2013).

[94] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 3 (Jan. 15, 2014), available at https://goo.gl/0RCC9E.

In order to deter the Commission from taking advantage of this frequent judicial deference by imposing such disconnected "fencing-in" remedies in non-fraud cases — which, of course, is compounded by the fact that most cases are never reviewed by courts at all — Congress should consider imposing some sort of minimal requirement that provisions in proposed orders and consent decrees be (i) reasonably related to challenged behavior, and (ii) no more onerous than necessary to correct or prevent the challenged violation.

H. Closing Letters

While consent decrees might help companies understand what the FTC will deem illegal on a case-by-case basis, in unique fact patterns, closing letters could do the inverse, telling companies what the FTC will deem *not* to be illegal, which is potentially far more useful in helping companies plan their conduct. In the past, the FTC issued at least a few closing letters with a meaningful degree of analysis of the practices at issue under the doctrinal framework of Section 5(n).[95] But in recent years, the FTC has markedly changes its approach, issuing fewer letters and writing those it did issue at a level of abstraction that offers little real guidance and even less analysis.[96]

Rep. Brett Guthrie's (R-KY) proposed CLEAR Act (H.R. 5109) would require the FTC to report annually to Congress on the status of its investigations, including the legal analysis supporting the FTC's decision to close some investigations without action. This requirement would not require the Commission to identify its targets, thus preserving the anonymity of the firms in question.[97] Most importantly, the bill requires:

> (1) IN GENERAL.—The Commission shall, on an annual basis, submit a report to Congress on investigations with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of subsection (a)(1)), detailing—
>
> > (A) the number of such investigations the Commission has commenced;
> >
> > (B) the number of such investigations the Commission has closed with no official agency action;

[95] *Id.* at 40-43. *See, e.g.,* Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf .

[96] *See, e.g*., Letter from Maneesha Mithal, Associate Director of Fed. Trade Comm'n to Lisa J. Sotto, Counsel to Michael's Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-storesinc./120706michaelsstorescltr.pdf.

[97] The Clarifying Legality and Enforcement Action Reasoning Act, H.R. 5109, 114th Cong. (2016) [hereinafter CLEAR Act] available at https://www.congress.gov/bill/114th-congress/house-bill/5109/text.

> (C) the disposition of such investigations, if such investigations have concluded and resulted in official agency action; and
>
> (D) for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal ***and economic*** analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

This bill, with our proposed addition noted, would go a long way to improving the value of the FTC's guidance. Indeed, such annual reporting could form annual addenda to guidance that the FTC issues in the guidance it provides on informational injury modeled on the Green Guides. Although the Green Guides themselves do not involve such reporting, it would make sense in this context, where the FTC is regularly confronted with far more novel fact patterns each year.

I. Re-opening Past Settlements

The FTC may, under its current rules, re-open past settlements at any time — subject only to the Commission's assertion about what the "public interest" requires and after giving companies an opportunity to "show cause" why their settlements should *not* be modified.[98] By contrast, courts require far more for re-opening their orders. The FTC has, in fact, proposed to re-open four settlements entered into in 2013 under the Green Guides. Congress should write a meaningful standard by which the FTC should have to justify re-opening past settlements. If the Commission continues on its current course, it will be able to use its settlements to bypass the procedural safeguards of notice-and-comment rulemaking.

III. Reasonable Siblings: Background on Section 5 and Negligence

The FTC's enforcement authority is derived from Section 5 of the Federal Trade Commission Act (FTC Act), which declares unlawful "[u]nfair methods of competition in or affecting commerce" and "unfair or deceptive acts or practices in or affecting commerce."[99] Under the broad terms of Section 5, the FTC challenges "unfair methods of competition" through their

[98] 16 C.F.R. 3.72(b).

[99] 15 U.S.C.A. § 45 (West 2017).

antitrust division and "unfair or deceptive practices" through their consumer protection division.[100] In pursuing its consumer protection mission there are different standards for "unfair" and "deceptive" practices, with its unfairness authority being "the broadest portion of the Commission's statutory authority."[101] Indeed, this "unfairness" authority was initially unrestrained by any statutory definition,[102] and remained so until Congress added Section 5(n) in 1994. In addition to Section 5 authority, however, the FTC has also asserted violations of other statutes in its data security enforcement, most notably the Gramm-Leach-Bliley Act ("GLBA"),[103] Children's Online Privacy Protection Act ("COPPA"),[104] as well as regulations promulgated under those statutes.[105]

Congress intentionally framed the FTC's authority under Section 5 in the general terms "unfair" and "deceptive" to ensure that the agency could protect consumers and competition throughout all trade and under changing circumstances.[106] To be sure, this broad authority has not been lost on the FTC, who readily acknowledges that "Congress intentionally framed the statute in general terms," which the agency interprets to mean "[t]he task of identifying unfair methods of competition" as being "assigned to the Commission."[107] Despite the addi-

---

[100] *See generally* Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law,* 101 Iowa L. Rev. 955, 964 (2016) (discussing in great lengths the FTC's "common law" approach) [hereinafter Hurwitz, *Uncommon Law*].

[101] *Id*.

[102] *See Id*.; *see also* Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) (setting the three-factor contours of the "unfairness" prong for the first time through application of Section 5 to cigarette advertisements).

[103] *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (2012) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to … protect the security and confidentiality of … customers' nonpublic personal information.").

[104] The Child Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, *et seq* (1994 & Supp. IV 1998) (making it unlawful under § 6502(a)(1) "for an operator of a website or online service directed to children … to collect personal information form a child in a manner that violates the regulations prescribed under subsection (b) of this section."); *see also* Melanie L. Hersh, Is Coppa A Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet, 28 Fordham Urb. L.J. 1831, 1878 (2001) (detailing how the FTC uses COPPA to regulate data security for children).

[105] *See, e.g.,* FTC Final Rule, 16 C.F.R. §§ 313.10–313.12 (2000); *Individual Reference Servs. Grp., Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 20 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. F.T.C.*, 295 F.3d 42 (D.C. Cir. 2002) (holding that the FTC's final rule, promulgated under the GLBA "did not contravene plain meaning of Act and were permissible construction of that legislation" and "agencies' action in promulgating final rules was not arbitrary and capricious").

[106] *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (observing if Congress "were to adopt the method of definition, it would undertake an endless task").

[107] Joshua D. Wright, Commissioner, Federal Trade Comm'n, Section 5 Recast: Defining the Federal Trade Commission's Unfair Methods of Competition Authority at the Executive Committee Meeting of the New York

tion of Section 5(n) to the Act in 1994 to *require* cost-benefit analysis, this lack of clear statutory guidance as to what constitutes "unfair" proved to be problematic, with at least one Commissioner recently recognizing that "nearly one hundred years after the agency's creation, the Commission has still not articulated what constitutes … unfair… leaving many wondering whether the Commission's Section 5 authority actually has any meaningful limits."[108] Commissioner Wright was referring to a lack of clarity around the meaning of unfairness in competition cases, but his point holds more generally.

Given the broad nature of Section 5, few industries are beyond the FTC's reach and the FTC has met the broad statutory language with an equally broad exercise of its authority to enforce Section 5.[109] The FTC has brought data security and privacy actions against advertising companies, financial institutions, health care companies, and, perhaps most significantly, companies engaged in providing data security products and services.[110] Further, not only are companies responsible for safeguarding their own data, but the FTC has also alleged that companies are responsible for any data security failings of their third-party clients and vendors, too.[111]

Companies who are the victims of such cyber-attacks are victims themselves. They suffer immense financial losses, stemming largely from reputational damage as customers are fearful of remaining loyal to companies who can't protect their personal and financial information.[112] According to one study, 76% of customers surveyed said they "would move away from companies with a high record of data breaches," with 90% responding that "there are

---

State Bar Association's Antitrust Section, 2 (June 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/section-5-recast-defining-federal-trade-commissions-unfair-methods-competition-authority/130619section5recast.pdf.

[108] *Id*.

[109] *See* Cho & Caplan, *Cybersecurity Lessons*; Stuart L. Pardau & Blake Edwards, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity 12 J. Bus. & Tech. L. 227, 232 (2017) (discussing the FTC's enforcement of "everything from funeral homes, vending machine companies, telemarketing and mail marketing schemes, credit reporting, and the healthcare industry.") [hereinafter Pardau & Edwards, *New Legal Frontiers*].

[110] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[111] *See id.* (For example, the consent decree agreed to in the FTC's enforcement action against Ashley Madison required the defendants to implement a comprehensive data-security program, including third-party assessments).

[112] *See generally* PONEMON, DATA BREACH; *see also Data breaches cost US businesses an average of $7 million – here's the breakdown*, Business Insider (April 27, 2017), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4 (providing that the average cost of a data security breach is $7 million, with 76% of customers saying they would move away from companies with a high record of data breaches).

apps and websites that pose risks to the protection and security of their personal information."[113] Unquestionably, data security is the cornerstone of the digital economy and digitization of the physical economy. As Naveen Menon, President of Cisco Systems for Southeast Asia, put it "[s]ecurity is what protects businesses, allowing them to innovate, build new products and services."[114]

The recent Equifax breach illustrates just how strongly reputational forces encourage companies to invest in data security. As of the time this testimony was being written, Equifax's post-hack stock had plummeted 30%.[115] Given the enormous stakes for companies' brands, it is not difficult to understand why—with no clear guidance from Congress or the FTC—companies have opted to settle and enter into consent decrees rather than risk further reputational damage and customer loss through embarrassing and costly litigation.[116] Out of approximately 60 data security enforcement actions, only two defendants dared face an FTC armed with near absolute discretion as to the interpretation of "reasonable" data security practices. This hesitation to challenge the FTC in order to gain clarity from the courts about what actually constitutes unreasonable practices — in addition to the more obvious reason of escaping liability — was only reinforced by the *LabMD* case, where the company's decision to litigate against the FTC rather than enter into a consent decree led to its demise.[117]

Data security poses a unique challenge: unlike other unfairness cases, the company at issue is both the victim (of data breaches) and the culprit (for allegedly having inadequate data security). In such circumstances, the FTC should apply unfairness as more of a negligence standard than strict liability. Consider both a company that has been hacked and a business owner whose business has burned down. In both situations, it is very likely that employees and customers lost items they consider to be precious — perhaps even irreplaceable. Additionally, it is equally likely that neither *wanted* this unfortunate event to occur. Finally, in both situations, prosecutors would investigate the accident to determine the cause and as-

---

[113] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vansonbourne.com/client-research/18091501JD.

[114] Naveen Menon, *There can be no digital economy without security*, World Economic Forum (May 8, 2017), https://www.weforum.org/agenda/2017/05/there-can-be-no-digital-economy-without-security/.

[115] *See, e.g.*, *Equifax Plummets After Huge Data Breach, Kroger Sinks on Profit drop, American Outdoor Brand Falls,* Yahoo Finance, Sept. 8, 2017, https://finance.yahoo.com/news/equifax-plummets-huge-data-breach-kroger-sinks-profit-drop-american-outdoor-brands-falls-144654294.html.

[116] *Id.*

[117] *Id.*

sess the damage and costs. However, under the FTC's current approach to Section 5 enforcement, how each business owner would be judged for liability purposes would vary greatly despite these similarities.

Under the common law of torts, absent some criminal intent (*e.g.*, insurance fraud) the businessman whose office burned down would only be held liable if he acted negligent in some way. At common law, negligence involves either an act that a *reasonable* person would know creates an unreasonable risk of harm to others.[118] Should a prosecutor or third party bring a lawsuit against the business owner, they would be required to put forth expert testimony and a detailed analysis showing exactly *how* and *why* the owner's negligence caused the fire.

Conversely, despite all of the FTC's rhetoric about "reasonableness" — which, as one might "reasonably" expect, should theoretically resemble a negligence-like framework — the FTC's approach to assessing whether a data security practice is unfair under Section 5 actually more closely resembles a rule of strict liability.[119] Indeed, rather than conduct any analysis showing that (1) the company owed a duty to consumers and (2) *how* that the company's breach of that duty was the cause of the breach — either directly or proximately— which injured the consumer, instead, as one judge noted, the FTC "kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…."[120]

There is no level of prudence that can avert *every* foreseeable harm. A crucial underpinning of calculating liability in civil suits is that some accidents are unforeseeable, some damages fall out of the chain of causation, and mitigation does not always equal complete prevention. Thus our civil jurisprudence acknowledges that no amount of care can prevent *all* accidents (fires, car crashes, *etc*.), or at least the standard of care required to achieve an accident rate near zero would be wildly disproportionate, paternalistic, and unrealistic to real-world applications (*e.g.*, setting the speed limit at 5 mph).

The chaos theory also applies to the unpredictability of data breaches. Thus, if the FTC wants to regulate data security using a "common law" approach, then it must be willing to accept that certain breaches are inevitable and liability should only arise where the company was truly negligent. This is not simply a policy argument; it is the weighing of costs and benefits that Section 5(n) requires — at least in theory. Companies do not want to be hacked any

---

[118] *See* Restatement (Second) of Torts § 284 (1965).

[119] *See* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standard-Less Data Security Standard*, Journal of Law, Economics and Policy, Forthcoming (Aug. 31, 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041533.

[120] Transcript of Proceedings at 91, 94–95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014).)).

more than homeowners want their houses to burn down. The FTC should begin its analysis of data security cases with that incentive in mind, and ask whether the company has acted as a "reasonably prudent person" would.

This, then, presents the key question: what constitutes "reasonably prudent" data security and privacy practices for purposes of avoiding liability under Section 5? To help inform Congress — and, in turn, the FTC — on how to go about answering this question, the remainder of this testimony will focus on determining three key elements of this question: (1) the types of injuries that should merit the FTC's attention, (2) the analytical framework, built upon empirical research and investigations, which should determine what constitutes "reasonable," and (3) the pleading requirements to determine the specificity with which the FTC must state its claim in the first instance.

IV. Informational Injuries In Practice: Data Security & Privacy Enforcement to Date

In 2005, the FTC brought its first data security case premised solely on unfairness — against a company (BJ's Warehouse) not for violating the promises it had made to consumers, but for the underlying adequacy of its data security practices.[121] Whether this was a proper use of Section 5 is not the important question — although it is essential to note that *BJ's Warehouse* was the consent decree that launched the FTC's use of unfairness for data security.a thousand" more (or closer to "hundreds" in the context of privacy and data security). Even if one stipulates that the FTC could have, and likely *would* have, prevailed on the merits, had the case gone to trial, the important question is this: how might the Commission have changed its approach to data security? That question becomes even more salient if one tries to project back, asking what the Commission should have done then if it had known what we know today: that twelve years later, we would still not have a single tech-related unfairness case resolved on the merits (and only four that had made it to federal court).[122]

The Commission had, of course, asked Congress for comprehensive privacy legislation in 2000.[123] Besides asking again, what else could the Commission have done? It could have be-

[121] Fed. Trade Comm'n, *BJ's Wholesale Club Settles FTC Charges* (June 16, 2005), *available at* https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

[122] *See Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017); *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 253 (3d Cir. 2015); *LabMD, Inc. v. F.T.C.*, No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd,* 776 F.3d 1275 (11th Cir. 2015); *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[123] Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Market Place- A Report to Congress* (2000) [hereinafter Privacy Report].

gun a rulemaking under the Magnusson-Moss Act of 1975, subject to the procedural safeguards imposed by Congress in 1980 (after the FTC's abuse of its rulemaking powers in the intervening five years). But, as many have noted, it would be difficult to craft prescriptive rules for data security or privacy in any rulemaking, and the process would have taken several years.

There *was* a third way: the FTC could have sought public comment on the issues of data security and privacy, issued a guidance document, then repeated the process every few years to update the agency's guidance to reflect current risks, technologies, and trade-offs. In short, the Commission could have followed the model established by its Green Guides.

V. The Green Guides as Model for Empirically Driven Guidance

As the FTC proceeds with Chairman Ohlhausen's plans for a workshop on "informational injuries," it should consider its own experience with the Green Guides as a model. The parallel is not exact: the Guides focus entirely on deception, and primarily on consumer expectations, while the FTC's proposed "informational injuries" would involve both deception and unfairness. However, the Guides do still delve into substantiation of environmental marking claims, and, thus, the underlying merits of what companies were promising their customers. FTC guidance on the meaning of "informational injuries" in the context of data security and privacy would necessarily cover wider ground, ultimately attempting to understand harms as well as "reasonable" industry practices under both deception and unfairness prongs. Still, the Guides emphasis on empirical substantiation would serve the FTC well in attempting to provide a clearer analytical basis for *why* a practice or action is deemed to have caused "informational injury" in certain cases, rather than merely stating *what* practices the FTC has determined likely to cause such harm.

Though court guidance in this context may seem rarer than the birth of a giant panda, the Third Circuit nonetheless provided some insight into the value of previous FTC guidance — namely the FTC's 2007 guidebook titled "Protecting Personal Information: A Guide for Business," — in understanding harms and "reasonable" practices that constitute violations of Section 5.[124] Discussing this guidebook, which "describes a 'checklist[]' of practices that form a 'sound data security plan,'" the court notably found that, because "[t]he guidebook does not state that any particular practice is required by [Section 5]," it, therefore, "could not, on its own, provide 'ascertainable' certainty' of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[125] Despite this recognition, the court still noted that the

[124] *Wyndham*, 799 F.3d at 256.

[125] *Id*. at 256 n.21.

guidebook did "counsel against many of the specific practices" alleged in that specific case, and thus, provided sufficient guidance in that very narrow holding to inform the defendant of "what" conduct was not considered reasonable.[126] Specifically, the court noted that the guidebook recommended:

> [T]hat companies "consider encrypting sensitive information that is stored on [a] computer network ... [, c]heck ... software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through the firewall and what they will be allowed to see ... to allow only trusted employees with a legitimate business need to access the network." It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like ... the software's default password[ ] and other easy-to-guess choices." And it recommends implementing a "breach response plan," *id.* at 16, which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information."[127]

Most notably, nowhere in the court's discussion did it identify a single instance of the FTC explaining *why* a certain practice is necessary or reasonable; instead the FTC had merely asserted that companies should just accept the FTC's suggestions, without any consideration or analysis as to whether the immense costs that might be associated with implementing many of these practices are in the consumers' best interest. This is far from the weighing of costs and benefits that Section 5(n) requires. By comparison, the Green Guides, while focused on deception, reflect a deep empiricism about substantiation of environmental marketing claims, informed by a notice and comment process and distilled into clear guidance accompanied by detailed analysis.

While multi-national corporations such as Wyndham *might* (arguably) possess the resources to blindly implement any and all suggestions the FTC makes, and to follow the FTC's pronouncements in each consent decree, the economic principle of scarcity will inevitably require smaller businesses with vastly fewer resources to make difficult decisions as to which practices they should utilize to provide the greatest security possible with its limited resources. For example, using the list above, would a company with limited resources be acting "reasonable" if it implemented a "breach response plan," but failed to check *every* software vendors' website regularly for alerts? Further, would a company be engaging in "deceptive"

[126] *Id*. at 256-57.

[127] *Id.* (internal citations omitted).

practices if it failed to notify customers that, due to limited resources, it could only implement half of the FTC's recommended practices? The answer to these questions matter and will undoubtedly have significant consequences on how competitive small businesses remain in this country. As mentioned earlier, one study suggests that 76% of customers "would move away from companies with a high record of data breaches," with 90% responding that "there are apps and websites that pose risks to the protection and security of their personal information."[128] This shows that consumers are understandably concerned about how well a company protects their data. If a company is essentially required to choose between admitting that it lacks the resources to implement advanced security practices on par with large, established businesses, or risk an FTC action for "deception," how can any startup or small business expect to compete and grow in these polarizing circumstances?

Under the FTC's current enforcement standards, this all shows how easily small businesses may find themselves in a catch-22. On the one hand, if the business wishes to pretend it has the resources to implement the same data security standards as multi-national corporations in order to attract and maintain customers weary of their data being hacked, the business will be acting "deceptively" in the eyes of the FTC, and will be open to the costly litigation, reputational damage, and massive fines that come with it. On the other hand, if the small business wishes to be open and readily admit that, due to resource constraints, its data security practices are anemic when compared to multi-national corporations, it will be open to the loss of customers and businesses invariably linked to such claims. As this illustrates, how can any startup or small business expect to compete without the FTC providing guidance as to best practices based on empirical research — including economies of scale?

Thus, to ensure the ability of businesses to compete and make sound decisions as to the allocation of their finite resources, it is imperative that the FTC not only endeavor to provide guidance as to *what* practices are sound, but also explain *why* such practices are necessary, as well as "how much" is necessary, especially in relation to a business's size and available resources.

A. The Green Guides (1992-2012)

First published in 1992, the Guides represented the Commission's attempt to better understand a novel issue before jumping in to case-by-case enforcement. By 1991, it was becoming increasingly common for companies to tout the environmental benefits of their products. In some ways, these claims were no different from traditional marketing claims: the FTC's job was to make sure consumers "got the benefit of the bargain." But in other ways, it was less

[128] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vanson-bourne.com/client-research/18091501JD.

clear exactly what that "benefit" was — such as regarding recycling content, recyclability, compostability, biodegradability, refillability, sourcing of products, etc. Rather than asserting how much of each of these consumers *should* get, the Commission sought to ground its understanding of these concepts in empirical data about what consumers actually expected. As the Commission summarized its approach in the Statement of Basis and Purpose for the 2012 update:

> The Commission issued the Guides to help marketers avoid making deceptive claims under Section 5 of the FTC Act. Under Section 5, a claim is deceptive if it likely misleads reasonable consumers. Because the Guides are based on how consumers reasonably interpret claims, consumer perception data provides the best evidence upon which to formulate guidance. As EPA observed, however, perceptions can change over time. The Guides, as administrative interpretations of Section 5, are inherently flexible and can accommodate evolving consumer perceptions. Thus, if a marketer can substantiate that consumers purchasing its product interpret a claim differently than what the Guides provide, its claims comply with the law.[129]

Of course, as the Deception Policy Statement notes, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[130] Thus, the Commission immediately added the following:

> the Green Guides are based on marketing to a general audience. However, when a marketer targets a particular segment of consumers, such as those who are particularly knowledgeable about the environment, the Commission will examine how reasonable members of that group interpret the advertisement. The Commission adds language in Section 260.1(d) of the Guides to emphasize this point. Marketers, nevertheless, should be aware that more sophisticated consumers may not view claims differently than less sophisticated consumers. In fact, the Commission's study yielded comparable results for both groups.[131]

This bears emphasis because many speak of privacy-sensitive consumers as a separate market segment, and argue that we should apply deception in privacy cases based upon their expectations. But here, unlike in privacy, the Commission actually undertook empirical research — which turned not to support an idea that probably seemed intuitively obvious: that

---

[129] Fed Trade Comm'n, Statement of Basis and Purpose (2012 Update), *at* 24-25, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguidesstatement.pdf [hereinafter "Statement of Basis and Purpose"].

[130] Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1983), *at* 1, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[131] *See* Statement of Basis and Purpose, *at* 25.

more environmentally knowledgeable or "conscious" consumers had different interpretation of environmental marketing claims.

The Commission issued the first Green Guides in August 1992, thirteen months after two days of public hearings, including a 90-day public comment period in between. The Commission followed this process in issuing revised Green Guides in 1996, 1998, and 2012. So detailed was the Commission's analysis, across so many different fact patterns, that, while the 2012 Guides ran a mere 12 pages in the Federal Register,[132] the Statement of Basis and Purpose for them ran a staggering 314 pages.[133] In each update, the FTC explored how the previous version of the Guides addresses each, the FTC's proposal, comments received on the proposal and justification for the final rule. In short, the FTC was doing something a lot like rulemaking. Except, of course, the Guides are not themselves legally binding.

The FTC has never done anything even resembling this type of comprehensive guide for data security or privacy. Indeed, just this year, the FTC touted "a series of blog posts" as a grand accomplishment in the FTC's "ongoing efforts to help businesses ensure they are taking reasonable steps to protect and secure consumer data."[134] The FTC has regularly trumpeted its 2012 Privacy Report, but that document does something very different. Most notably, the Report calls on industry actors to self-police in the most general of terms, making statements like "to the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work."[135] Unlike the focus on substance and comprehensiveness of the Green Guides, the 2012 Privacy Report speaks in generalities, dictating "areas where the FTC will be active," such as in monitoring Do Not Track implementation or promoting enforceable self-regulatory codes.[136] The lack of a Statement of Basis and Purpose akin to that issued in updating the Green Guides (the 2012 Statement totaled a whopping 314 pages) introduces unpredictability into the enforcement process, and chills industry action on data security and privacy.

---

[132] 16 C.F.R. 260 (2012).

[133] *See generally* note *129*.

[134] Press Release, Fed. Trade Comm'n, Stick with Security: FTC to Provide Additional Insights on Reasonable Data Security Practices (July 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/stick-security-ftc-provide-additional-insights-reasonable-data.

[135] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), *at* 73, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. [hereinafter "2012 Privacy Report"].

[136] *Id.* at 72.

In all, the Green Guides offer a clear, workable model for how the FTC could provide empirically grounded guidance on data security and privacy — even without any action by Congress. The key steps in issuing such guidance would be:

1. Study current industry practices across a wide range of businesses;
2. Gather data on consumer *expectations*, rather than making assumptions about consumer preferences;
3. Engage the Bureau of Economics and the FTC's growing team of in-house technologists in analysis of the costs and benefits of practice; and
4. Issue (at least) biennial or triennial guidance to reflect the changing nature, degree, and applicability of data security and privacy regulations.

Short of rulemaking, this rulemaking-like approach offers the most clarity, comprehensibility, and predictability for both FTC enforcement staff and industry actors.

B. What the Commission Said in 2012 about Modifying the Guides

There is an obvious tension between conducting thorough empirical assessments to inform updating Commission guidance and how often that guidance can be updated: the more regular the update, the more difficult it will be to for the Commission to maintain methodological rigor in justifying that update. The 2012 Statement of Basis and Purpose noted requests that the Commission review and update the Guides every two or three years, but concluded:

> Given the comprehensive scope of the review process, the Commission cannot commit to conducting a full-scale review of the Guides more frequently than every ten years. The Commission, however, need not wait ten years to review particular sections of the Guides if it has reason to believe changes are appropriate. For example, the Commission can accelerate the scheduled review to address significant changes in the marketplace, such as a substantial change in consumer perception or emerging environmental claims. When that happens, interested parties may contact the Commission or file petitions to modify the Guides pursuant to the Commission's general procedures.[137]

This strikes a sensible balance. Unfortunately, this is not at all how the Commission has handled modification of the 2012 Green Guides. Within a year, the FTC would modify the Green guides substantially with no such process for empirical substantiation to justify the new change. And this year, not five years after the issuance of the Guides, it modified the Guides yet again.

[137] *See* Statement of Basis and Purpose, *at* 26-27.

VI. Eroding the Green Guides and their Empirical Approach

While the Green Guides offer a model for empirically grounded consumer protection, the Commission has gradually moved away from that approach since issuing its last update to the Green Guides in 2012 — following an approach that more closely resembles its approach to data security and privacy.

A. Modification of the Green Guides by Policy Statement (2013)

In 2013, FTC issued an enforcement policy statement clarifying how it would apply the Green Guides,[138] updated just the year after taking notice-and-comment, to architectural coatings such as paint. The Commission appended this Policy Statement onto its settlement with PPG Architectural Finishes, Inc. ("PPG") and The Sherwin-Williams Company ("Sherwin-Williams") to settle alleged violations of Section 5 for marketing paints as being "Free" of Volatile Organic Compounds (VOCs).[139] Specifically, the Policy Statement focused on application of the 2012 Green Guides' trace-amount test, which provided:

> Depending on the context, a free-of or does-not-contain claim is appropriate even for a product, package, or service that contains or uses a trace amount of a substance if: (1) the level of the specified substance is no more than that which would be found as an acknowledged trace contaminant or background level; (2) the substance's presence does not cause material harm that consumers typically associate with that substance; and (3) the substance has not been added intentionally to the product.[140]

The Policy Statement made two clarifications specific to architectural coatings:

> First, the "material harm" prong specifically includes harm to the environment and human health. This refinement acknowledges that consumers find both the environmental and health effects of VOCs material in evaluating VOC-free claims for architectural coatings.

---

[138] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings (Mar. 6, 2013), https://www.ftc.gov/sites/default/files/ documents/cases/2013/03/130306ppgpolicystatement.pdf.

[139] Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges Against The Sherwin-Williams Co. and PPG Architectural Finishes, Inc.; Issues Enforcement Policy Statement on "Zero VOC" Paint Claims (Mar. 6, 2013), https://www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-orderssettling-charges-against-sherwin.

[140] 16 C.F.R. § 260.9(c) (2012).

> Second, the orders define "trace level" as the background level of VOCs in the ambient air, as opposed to the level at which the VOCs in the paint would be considered "an acknowledged trace contaminant." The harm consumers associate with VOCs in coatings is caused by emissions following application. Thus measuring the impact on background levels of VOCs in the ambient air aligns with consumer expectations about VOC-free claims for coatings.[141]

In both respects, the Policy Statement amended the Green Guides — while purporting merely to mirror the Guides. Most notably, the Guides had always been grounded in claims about environmental harms. For example, the Statement of Basis and Purpose for the 2012 Update had said:

> In this context [the "free of" section of the Guides"], the Commission reminds marketers that although **the Guides provide information on making truthful environmental claims**, marketers should be cognizant that consumers may seek out free-of claims for non-environmental reasons. For example, as multiple commenters stated, chemically sensitive consumers may be particularly likely to seek out products with free-of claims, and risk the most grievous injury from deceptive claims.[142]

But now the FTC's enforcement framework would, for the first time, focus on "human health" as well. In principle, this is perfectly appropriate: after all, "Unjustified consumer injury is the primary focus of the FTC Act," as the Unfairness Policy Statement reminds us.[143] But note that the Commission was *not* bringing an unfairness claim — which would have required satisfying the cost-benefit analysis of Section 5(n). Instead, the Commission was bringing a pure deception claim, as with any Green Guides claim. But unlike deception cases brought under the Green Guides, the Commission provided none of the kind of empirical evidence about how consumers understood green marketing claims that had informed the Green Guides. The Commission did not seek public comment on this proposed enforcement policy statement, nor did it supply any such evidence of its own.

In short, the 2013 Policy Statement represented not merely a *de facto* amendment of the Green Guides, undermining the precedential value of the Guides and of all other FTC guidance documents, but a break with the empirical approach by which the FTC had developed

---

[141] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings, *at* 2, https://www.ftc.gov/sites/default/files/documents/public_statements/voc-free-claims-architectural-coatings/130306ppgpolicystatement.pdf.

[142] *See* Statement of Basis and Purpose, *at* 138 n. 469.

[143] 1980 Unfairness Policy Statement.

the Guides since 1992. This alone should call into question the FTC's willingness, in recent years, to ground consumer protection work in empirical analysis. But worse was yet to come.

B. Modification of the Green Guides by Re-Opening Consent Decree (2017)

This July, Ohlhausen, now Acting Chairwoman, effectively proposed amending the FTC's Green Guides — first issued in 1992 and updated in 1996, 1998 and 2012 — via proposed consent orders issued to four paint companies accused of deceptively promoting emission-free or zero volatile organic compounds in violation of Section 5 of the FTC Act.[144] In the corresponding press release, the Commission said it plans to "propose harmonizing changes to two earlier consent orders issued in the similar PPG Architectural Finishes, Inc. (Docket No. C-4385) and the Sherwin Williams Company (Docket No. C-4386) matters," and plans to "issue orders to show cause why those matters should not be modified pursuant to Section 3.72(b) of the Commission Rules of Practice, 16 C.F.R. 3.72(b)," if the consent orders are finalized.[145]

This repeated, and compounded, the two sins committed by the FTC in 2013: (1) undermining the value of Commission guidance (here, both the 2012 Guides and the 2013 Enforcement Policy Statement) by reminding all affected parties that guidance provided one day can be changed or revoked the next and (2) failing to provide empirical substantiation for its new approach. To these sins, the Commission added two more: (3) revoking guidance that had been treated as authoritative, and relied upon, by regulated parties for the previous four years through a consent decree and (4) re-opening the two consent decrees to which the 2013 Enforcement policy was attached to "harmonize" them with the FTC's new approach. Revoking guidance treated as authoritative raises fundamental constitutional concerns about "fair notice." Re-opening consent decrees raises even more serious concerns about the FTC's process.

These concerns are reflected in recently proposed FTC settlements. In the 2013 PPG and Sherwin-Williams consent orders, the Commission specified the scope of its jurisdiction in Article II of the orders, stating:

---

[144] Press Release, Fed. Trade Comm'n, Paint Companies Settle FTC Charges That They Misled Consumers; Claimed Products Are Emission- and VOC-free and Safe for Babies and other Sensitive Populations, (July 11, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/07/paint-companies-settle-ftc-charges-they-misled-consumers-claimed.

[145] *Id.* at ¶ 13.

> IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any covered product in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, regarding:
>
> A. The VOC level of such product; or
>
> B. Any other *environmental* benefit or attribute of such product,
>
> unless the representation is true, not misleading, and, at the time it is made, respondent possesses and relies upon competent and reliable scientific evidence that substantiates the representation.[146]

In the same orders, the Commission defined "trace" levels of VOCs as including a "human health" component, stating:

> 7. "Trace" level of VOCs shall mean:
>
> A. VOCs have not been intentionally added to the product;
>
> B. The presence of VOCs at that level does not cause material harm that consumers typically associate with VOCs, including but not limited to, harm to the environment or *human health*; and
>
> C. The presence of VOCs at that level does not result in concentrations higher than would be found at background levels in the ambient air.[147]

While the inclusion of language that specified health as a VOC-related hazard created no immediate substantive changes, it laid the groundwork for a broadening of what constitutes a legitimate claim under the definition of VOC. Specifically, this would mean that the FTC would only have to take one additional step to claim a VOC-related violation if a company did not meet some broad, amorphous standard of "human health" conceived by the FTC. In fact, the 2017 Benjamin & Moore Co., Inc., ICP Construction Inc., YOLO Colorhouse LLC, and Imperial Paints, LLC consent orders took this additional step in an updated Article II, stating:

> IT IS FURTHER ORDERED that Respondent …. must not make any representation, expressly or by implication … regarding:

---

[146] Fed. Trade Comm'n, *In the Matter of PPG Architectural Finishes, Inc.*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025ppgagree.pdf; *see also* Fed. Trade Comm'n, *In the Matter of Sherwin-Williams Company*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025sherwinwilliamsagree.pdf.

[147] *Id.* at 3.

A. The emission of the covered product;

B. The VOC level of the covered product;

C. The odor of the covered product;

D. *Any other health benefit or attribute* of, or risk associated with exposure to, the covered product, including those related to VOC, emission, or chemical composition; or

E. Any other environmental benefit or attribute of the covered product, including those related to VOC, emission, or chemical composition, unless the representation is non-misleading, including that, at the time such representation is made, Respondent possesses and relies upon competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence, to substantiate that the representation is true.

Given the nature and type of these products, it is possible that health-related hazards should have been included in these particular consent orders. This would imply that it is the specific context of these cases that serves as a justification for the inclusion of the health-related language. However, the harmonization of these new orders with the 2013 PPG and Sherwin-Williams orders would create new, broader obligations on those two companies. More generally, this would imply that the basis of the FTC's authority emanates not from the context in which the claim is brought, but instead from the very nature of VOCs, i.e. as newly-deemed health hazards.

As a general principle, this means that, under its deception authority, the FTC could create *ex post facto* justifications for expanding its enforcement powers arbitrarily and with no forward guidance. For example, although the voluminous 2012 Green Guides Statement of Basis and Purpose made no mention of health risks,[148] the Commission found a way to add it on to previous consent agreements in a unilateral, non-deliberative way. This places industry actors at the mercy of the FTC, which can alter previous consent orders based on present or future interpretations of "deception."

C. Remember Concerns over Revocation of the Disgorgement Policy?

It is ironic that it should be this particular FTC that would modify a Policy Statement, which was treated as authoritative by regulated parties for four years and which was itself a surreptitious modification of a Guide issued through public notice and comment (and resulting

[148] *See generally* Statement of Basis and Purpose.

in a 314-page Statement of Basis and Purpose), through such summary means — given that Acting Chairman Ohlhausen had previously urged greater deliberation and public input in withdrawing a policy statement.

In July 2012, the FTC summarily revoked its 2003 Policy Statement on Monetary Equitable Remedies in Competition Cases (commonly called the "Disgorgement Policy Statement")[149] on a 2-1 vote.[150] Commissioner Ohlhausen, the sole Republican on the Commission at the time, objected: "we are moving from clear guidance on disgorgement to virtually no guidance on this important policy issue."[151] She also objected to the cursory, non-deliberative nature of the underlying process:

> I am troubled by the seeming lack of deliberation that has accompanied the withdrawal of the Policy Statement. Notably, the Commission sought public comment on a draft of the Policy Statement before it was adopted. That public comment process was not pursued in connection with the withdrawal of the statement. I believe there should have been more internal deliberation and likely public input before the Commission withdrew a policy statement that appears to have served this agency well over the past nine years.[152]

What then-Commissioner Ohlhausen said then about revocation of a policy statement remains true now about substantial modification of a policy statement (which is effectively a partial withdrawal of previous guidance): both internal debate and public input are essential. Burying the request for public comment in a press release about new settlements hardly counts as an adequate basis for reconsidering the 2013 Policy Statement — let alone modifying the 2012 Green Guides.

D. What Re-Opening FTC Settlements Could Mean for Tech Companies

The Commission could have, at any time over the last twenty years, undertaken the kind of empirical analysis that led to the Green Guides, and published guidance about interpretation of Section 5, but never did so. Instead, the Commission issued only a series of reports making broad, general recommendations. In fact, in one of the only two data security cases not to

---

[149] Fed. Trade Comm'n, Policy Statement on Monetary Equitable Remedies in Competition Cases, 68 Fed. Reg. 45,820 (Aug. 4, 2003).

[150] Press Release, Fed. Trade Comm'n, FTC Issues Policy Statement on Use of Monetary Remedies in Competition Cases (July 31, 2003), available at http://www.ftc.gov/opa/2003/07/disgorgement.shtm.

[151] *See* Statement of Commissioner Maureen K. Ohlhausen Dissenting from the Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases, *at* 2 (July 31, 2012), https://www.ftc.gov/public-statements/2012/07/statement-commissioner-maureen-k-ohlhausen-dissenting-commissions-decision.

[152] *Id.* at 2.

end in a consent decree, a federal district judge blasted the FTC's decision not provide *any* data security standards:

> No wonder you can't get this resolved, because if [a 20-year consent order is] the opening salvo, even I would be outraged, or at least I wouldn't be very receptive to it if that's the opening bid…. You have been completely unreasonable about this. And even today you are not willing to accept any responsibility…. *I think that you will admit that there are no security standards from the FTC*. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…. [H]ow does any company in the United States operate when . . . [it] says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did…. *[Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required*. You are a regulatory agency. I suspect you can do that.[153]

In recent years, the Commission has proudly trumpeted its "common law of consent decrees" as providing guidance to regulated entities.[154] Now, everyone must understand that those consent decrees may be modified at any time, particularly those consent decrees that are ordered by the Commission (as opposed to a federal court). As the Supreme Court made clear, "[t]he Commission has statutory power to reopen and modify its orders at all times."[155] In order to reopen and modify an order, the Commission faces an incredibly low bar, having to merely show that it has "reasonable grounds to believe that public interest at the present time would be served by reopening."[156] Meanwhile, the FTC's consent decrees often stipulate that the defendant "waives… all rights to seek judicial review or otherwise challenge or contest the validity of the order entered pursuant to this agreement."[157]

---

[153] Transcript of Proceedings at 91, 94-95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014)) (emphasis added).

[154] Julie Brill, Comm'r, Fed. Trade Comm'n, "Privacy, Consumer Protection, and Competition," Address at the 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-and-competition/120427loyolasymposium.pdf (stating the FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow").

[155] Atl. Ref. Co. v. F.T.C., 381 U.S. 357, 377 (1965).

[156] *Elmo Co. v. F.T.C.*, 389 F.2d 550, 552 (D.C. Cir. 1967), *cert. denied*, 392 U.S. 905 (1968).

[157] *See, e.g.,* Agreement Containing Consent Order at 3(C), In re Oracle, No. 132 3115 (F.T.C. Dec. 21, 2015), https://www.ftc.gov/system/files/documents/cases/151221oracleorder.pdf.

But in cases where the FTC needs a court to issue a consent decree (e.g., to obtain an injunction or restitution), if the FTC wishes to modify the decree, it must at least meet the requirements imposed by Federal Rule of Civil Procedure 60:[158] the FTC must meet a heightened pleading standard through a showing of, for example, "fraud," "mistake," or "newly discovered evidence" necessitating such a modification.[159] Furthermore, the FTC does not have the freedom to modify court ordered consent decrees "at any time," as with settlements, but must file a motion "within a reasonable time" — the same standard that applies to all litigants in federal court.[160]

Why should there be such radically different standards? It is true that violating court-ordered consent decrees can result in criminal liability penalties, while violating Commission-ordered consent decrees means only civil penalties — but those penalties may be significant. For example, in 2015, the FTC imposed a $100 million fine against Lifelock for violating a 2010 consent decree by failing to provide "reasonable" data security[161] — over eight times the amount of the company's 2010 settlement and two thirds of the company's entire revenue that quarter ($156.2 million).[162] In general, arbitrarily-imposed, post-hoc civil liability carries the risk of causing significant economic loss, reputational harm, and even business closure. For example, the Commission could re-open *all* its past data security and privacy cases to modify the meaning of the term "covered information." To the extent that companies are found to be in non-compliance with the new standard, they would be liable for prosecution to the full extent of the FTC's powers. Besides compromising the ability of existing industry actors to comply, invest, and grow, this would have the effect of deterring new actors from entering a data-based industry for fear of uncertainty and retroactive prosecution.

Congress should reassess the standard by which the FTC may reopen and modify its own orders. In doing so, it should begin with the question articulated long ago by the Supreme Court: "whether any thing has happened that will justify … changing a decree."[163] In answering this question, the Court made clear that "[n]othing less than a clear showing of grievous

---

[158] Fed. R. Civ. P. 60 (stating that "the court may relieve a party or its legal representative from a final judgment, order, or proceeding" for certain reasons, including "mistake," "newly discovered evidence," "fraud," and "any other reason that justifies relief.").

[159] Fed. R. Civ. P. 60(b).

[160] Fed. R. Civ. P. 60(c).

[161] Fed. Trade Comm'n, *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order* (Dec. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

[162] LifeLock, Inc., *LifeLock Announces 2015 Fourth Quarter Results* (Feb. 10, 2016), *available at* https://www.lifelock.com/pr/2016/02/10/lifelock-announces-2015-fourth-quarter-results-2/

[163] *United States v. Swift & Co*., 286 U.S. 106, 119 (1932).

wrong evoked by new and unforeseen conditions should lead us to change what was decreed ... with the consent of all concerned."[164] The reason for the Court's hesitation to modify consent decrees should be obvious: despite retaining the force of a court order, consent decrees are, at their core, stipulated terms *mutually* agreed to by the parties to the litigation, similar to traditional settlements of civil litigation. Thus, by choosing to settle and enter into consent decrees, "[t]he parties waive their right to litigate the issues involved in the case and thus save themselves the time, expense, and inevitable risk of litigation."[165]

In federal court, Rule 60 forces parties to show that circumstances have indeed changed enough to justify modification of a court order. However, having to only show that it believes the "public interest" would be served, the FTC essentially is not required to make *any* showing of necessity that would counterbalance the value of preserving the terms of the settlement. Given the enormous weight the FTC itself has placed upon its "common law of consent decrees," as a substitute both for judicial decisions and clearer guidance from the agency, Congress should find it alarming that the FTC is now undermining the value of that pseudo-common law.

Ultimately, allowing the FTC to modify such agreements without showing any real cause not only negates the value of such agreements to each company (in efficiently resolving the enforcement action and allowing the company to move on), but more systemically and perhaps more importantly, it diminishes the public's trust in the government to be true to its word. Procedure matters. When agencies fail to utilize fair procedures in developing laws, the public's faith in both the laws and underlying institutions is diminished. This, in turn, undermines their effectiveness and further erodes the public's trust in the legal institutions upon which our democracy rests.[166] Thus, even in instances where the policy behind the rule may be sound, a failure by the implementing agency to follow basic due process will undermine the public's faith and deprive businesses of the certainty they need to thrive.[167]

---

[164] *Id*.

[165] *Local No. 93, Int'l Asso. of Firefighters, etc. v. Cleveland*, 478 U.S. 501, 522 (1986) (quoting *United States v. Armour & Co.*, 402 U.S. 673, 681-682 (1971)).

[166] *See, e.g*, Pew Research Center, Beyond Distrust: How Americans View Their Government (2015) ("Only 19% of Americans today say they can trust the government in Washington to do what is right "just about always" (3%) or "most of the time" (16%).").

[167] *See, e.g., Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974) (recognizing that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible).

VII. Better Empirical Research & Investigations

Why *doesn't* the FTC do more empirical research — the kind that went into the Green Guides? What should the process around, and following, its forthcoming workshop on "informational injuries" look like?

A. What the FTC Does Now

Since 2013, the FTC has published each January an annual report titled the "Privacy & Data Security Update."[168] The 2016 Report[169] boasts the FTC's "unparalleled experience in consumer privacy enforcement[170]" and the wide spectrum of offline, online, and mobile privacy practices that the Commission has addressed with enforcement actions:

> [The FTC] has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.[171]

Given the far-reaching scope of the FTC's jurisdiction on Section 5 enforcement and the wide range of companies that have settled "informational injury" cases, one might expect the these annual "Updates" to do more than merely summarize the previous year's activities, and instead provide empirical research into the privacy and data threats facing consumers. By failing to do so, the Commission not only leaves businesses in the dark as to what constitutes "reasonable" practices in the Government's eyes, but fails to inform them of the best practices available to ensure that Americans' data and privacy is adequately protected.

For example, if the Commission is to proudly report that consumer protection was achieved from settling charges with a mobile ad network on the grounds that "[the company] deceived consumers by falsely leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones,"[172] that Commission's work should not have ended there as a single bullet-point of the Commission's many highlights. As an

---

[168] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2013 (June 2012), *available at* https://www.ftc.gov/policy/reports/policy-reports/commission-and-staff-reports?title=data+security&items_per_page=20.

[169] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2016 (Jan 2017), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2016.

[170] *Id*. *at* 2.

[171] *Id*.

[172] *Id.*

enforcement agency with vast interpretive powers on deceptive practices, and an investigative body with considerable analytical resources, the Commission has a further duty to clearly explain the empirical rationale that substantiates the settlement: Just how do consumers understand privacy in the use of advertising cookies? How might companies use Do Not Track signals, given those consumer expectations, to provide an effective opt-out mechanism? How should the standard differ based on the sizes of companies and the services they provide? What "informational injuries" occur when consumers unknowingly receiving tailored advertisements through the use of unique device identifiers? It is one thing to say that the Commission should not have to answer all these questions in its pleadings, or even in order to prevail in a deception case. It is quite another to say that the Commission should not be expected to perform any research even after the fact, especially on matters that recur across a larger arc of enforcement actions.

Unforeseen vulnerabilities are the inevitable side-effect of rapid technological advancements; in the area of data privacy and security, new consumer risks will arise continually, raising questions that *should* merit careful quantitative and qualitative analyses. However, in its "Privacy & Data Security Update," the FTC essentially asserts an answer without "showing its work."

This is in stark comparison to the FTC's approach on the Green Guides, where "the Commission sought comment on a number of general issues, including the continuing need for, and economic impact of, the Guides, as well as the Guides' effect on environmental claims":[173]

> [B]ecause the Guides are based on consumer understanding of environmental claims, consumer perception research provides the best evidence upon which to formulate guidance. The Commission therefore conducted its own study in July and August of 2009. The study presented 3,777 participants with questions calculated to determine how they understood certain environmental claims. The first portion of the study examined general environmental benefit claims ("green" and "eco-friendly"), as well as "sustainable," "made with renewable materials," "made with renewable energy," and "made with recycled materials" claims. To examine whether consumers' understanding of these claims differed depending on the product being advertised, the study tested the claims as they appeared on three different products: wrapping paper, a laundry basket, and kitchen flooring. The second portion of the study tested carbon offset and carbon neutral claims.[174]

Here is an excellent example of the FTC's use of consumer perception data to study the effect of environmental labels, with variables on consumer behavioral segments and changes on

[173] Statement of Basis and Purpose, *at* 8.

[174] *Id.* at 9-10.

perception over time, to substantiate deception claims. Even with the empirical research grounded in a large sample size, the Commission continued to reanalyze "claims appearing in marketing on a case-by-case basis because [the Commission] lacked information about how consumers interpret these claims."[175] The "Green Guides: Statement of Basis and Purpose"[176] is a 314 page document that comprehensively reviews the Commission's economic and consumer perception studies and weighs different empirical methodologies on the appropriate model of risk assessment. It meaningfully fleshes out the Green Guides' core guidance on the "(1) general principles that apply to all environmental marketing claims; (2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and (3) how marketers can qualify their claims to avoid deceiving consumers," with self-awareness of the economic impact of regulations and a robust metric on consumer expectations to materialize the Commission's enforcement policies.

It is deeply troubling that this level of thoroughness evades the Commission's privacy enforcement, where the toolbox of economics remains unopened in managing the information flows of commercial data in boundless technology sectors pervading everyday life. The FTC's history of consent decrees provides nothing more than anecdotal evidence that *some* guiding principle is present, within the vague conceptual frameworks of "privacy by design," "data minimization", or "notice and choice."[177]" Data privacy and security regulations do not exist in a silo, abstracted and harbored from real-life economic consequences for the consumers, firms, and stakeholders—whose interests intersect at the axis of the costs and benefits of implementing privacy systems, the need for working data in nascent industries, and the market's right to make informed decisions. Consumer protection through privacy regulation is undoubtedly a matter of economic significance parallel to antitrust policies or the label marketing in the Green Guides. Personally identifiable information ("PII") is a valuable corporate asset like any other,[178] with competitive market forces affecting how it is processed, shared, and retained. Modern consumers are cognizant of the tradeoffs they make at the convenience of integrated technology services, and the downstream uses of their data. Accordingly, not every technical deviation from a company's privacy policy is an affront to consumer welfare that causes "unavoidable harms not outweighed by the benefits to consumers or competition."[179] The FTC has too long failed to articulate the privacy risks it intends to rectify, nor to

[175] *See* Statement of Basis and Purpose, *at* 27.

[176] *See generally* Statement of Basis and Purpose.

[177] *See generally* 2012 Privacy Report.

[178] Clearwater Compliance LLC, *The Clearwater Definition of an Information Asset*, https://clearwatercompliance.com/wp-content/uploads/2015/11/Clearwater-Definition-of-Information-Assets-with-Examples_V8.pdf.

[179] 12 U.S.C. § 5331(c)(1).

quantify the "material" consumer harm through behavioral economics or any empirical metric substantiated beyond its usual *ipso facto* assertion of deception.

B. The Paperwork Reduction Act

A noteworthy legislation that defined the FTC's administrative authority after Congress imposed additional safeguards upon the FTC's Magnuson-Moss rulemaking powers in 1980 is the Paperwork Reduction Act of 1980 ("PRA").[180] These two 1980 enactments must be understood together as embodying Carter-era attempts to reduce the burdens of government. Specifically, Congress intended the PRA to serve as an administrative check on the Federal agency's information collection policy, with the goal of reducing paperwork burdens for individuals, businesses, and nonprofits by requiring the FTC to seek clearance from the Office of Management and Budget ("OMB") on compulsory process orders surveying ten or more members of the public.

The "collection of information" that falls under the constraints of the PRA is defined as:

> the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either— answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States.[181]

Some have claimed that the PRA has hampered the FTC's ability to collect data from companies and thus to perform better analysis of industry practices, informational injuries, and the like. The FTC's power to gather information *without* "a specific law enforcement purpose" derives from Section 6(b) of the FTC Act, which the FTC has summarized in relevant part as follows:

> Section 6(b) empowers the Commission to require the filing of "annual or special reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of the entities to whom the inquiry is addressed. [182]

---

[180] Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501–3520 (2012)).

[181] 44 U.S.C. § 3502(3).

[182] Fed. Trade Comm'n, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (July 2008), *available at* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

Such reports would certainly be helpful for providing better substantiated guidance regarding data privacy and security practices. It is worth carefully considering what the PRA requires and how it might affect the FTC's collection of data. There is indeed some circumstantial evidence to suggest that the FTC may be structuring its 6(b) inquiries to avoid the PRA, by limiting the number of firms from which the FTC requests data to fewer than ten[183] — the threshold for triggering the PRA's requirements.

A case study on the FTC's survey of Patent Assertion Entities ("PAEs")[184] illustrates two potential ways the PRA might affect the FTC's collection of empirical data and thus the quality of its analysis and guidance in data security and privacy cases. First, by its own terms, the PRA applies even to *voluntary* data-collection of the sort that could allow the FTC compile "line of business" studies that consider wider practices beyond a single case:

> [T]he obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency … *whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit.*[185]

The burden-minimization goal of the PRA is evaluated by the OMB based on broad, unpredictable criteria, such as whether the "the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility."[186] The PRA has been enforced by the OMB with tunnel vision on reducing the burden of paperwork and compliance, measured quite simply on the metric of man hours spent processing the paperwork.[187] However, the more important question lies on balancing the potential burden of information collection with the value of added research and empirical data on FTC policymaking. The balance was correctly struck on the Green

---

[183] *See e.g.*, FTC To Study Credit Card Industry Data Security Auditing Commission Issues Orders to Nine Companies That Conduct Payment Card Industry Screening (March 2016) https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing;
FTC To Study Mobile Device Industry's Security Update Practices (May 2016) https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[184] Layne-Farrar, Anne, What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016). Available at SSRN: https://ssrn.com/abstract=2722057. or http://dx.doi.org/10.2139/ssrn.2722057.

[185] 5 C.F.R. § 1320.3(c).

[186] United States Office of Personnel Management, Paperwork Reduction Act (PRA) Guide Version 2.0 (April 2011), available at https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

[187] *Id. See also* Sam Batkins, Evaluating the Paperwork Reduction Act: Are Burdens Being Reduced? AAF, https://www.americanactionforum.org/testimony/evaluating-paperwork-reduction-act-burdens-reduced/.

Guides, where the PRA analysis was satisfied upon a consideration of the benefits of consumer surveys which outweighed the minimal burdens to the respondents:

> Overall burden for the pretest and questionnaire would thus be 2,511 hours. The cost per respondent should be negligible. Participation is voluntary and will not require start-up, capital, or labor expenditures by respondents.[188]

Moreover, the FTC integrated various suggestions on the study methodology and data collection methods submitted in a public comment by the General Electric Company ("GE"), to ensure that the Commission surveyed "a proper universe of consumers" upon which to "obtain accurate projections of national sentiment."[189]

> With respect to GE's concern about identifying the ''proper universe of consumers,'' FTC staff has included in the questionnaire a brief section of questions that address participants' level of interest in environmental issues. For example, one question asks: ''In the past six months, have you chosen to purchase one product rather than another because the product is better for the environment?'' Through analyses of answers to such questions, staff can compare the study responses of participants who have a high degree of interest in environmental issues and who take these issues into account when making purchasing decisions with responses of participants who are not as concerned with environmental issues.
>
> GE also asserts that the FTC should ensure a ''proper sample size.'' The FTC staff determined the sample size of 3,700 consumers based on several considerations, including the funds available for the study, the cost of different sample size configurations, the number of environmental claims to be examined, and a power analysis. In this study, 150 participants will see each of the various environmental marketing claims to be compared. Staff believes that this will be adequate to allow comparisons across treatment cells.[190]

By contrast, the FTC study on PAEs, which also received PRA clearance, compiled "nonpublic data on licensing agreements, patent acquisition practices, and related costs and revenues"[191] to illuminate how PAEs operate in patent enforcement activity outside the confines

---

[188] Fed. Trade Comm'n, Agency Information Collection Activities; Submission for OMB Review; Comment Request (May 2009), Federal Register / VOL. 74, NO. 90, *available at* https://www.ftc.gov/sites/default/files/documents/federal_register_notices/green-marketing-consumer-perception-study-agency-information-collection-activities-submission-omb/090512greenmarketing.pdf.

[189] *Id* at 22398.

[190] *Id*.

[191] *See* What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016); "Supporting Statement for a Paperwork Reduction Act: Part B" *available at* http://www.reginfo.gov/public/do/DownloadDocument?objectID=47563401.

of litigation records. But even when the OMB cleared the PAE study, the FTC chose a limited sample size of "25 PAEs, 9 wireless chipset manufacturers that hold patents, and 6 non-practicing wireless chipset patent holders."[192] This restrictive sample size significantly limited the applicability of the Commission's conclusions. More broadly, it suggests a shift towards a general reluctance to design and implement systemic research even when the required administrative blessing is obtained under the PRA.

The PRA Guide of 2011 outlines information collection policies and procedures, albeit with only a superficial explanation of statistical methodologies, and zero mention of survey design and quantitative research methods. [193] It is a cause for concern that the OMB's task of cutting down on the amount of paperwork is framed so parochially, for the short term goal of reducing participation hours, without perhaps considering cases where the quality and usability of the research itself depends on obtaining a larger sample. The mandate to limit the sample size of survey respondents ironically defeats the "practical utility" of the research, which is one of the main cornerstones of the PRA.

On the other hand, the PRA does not apply to *all* voluntary collection — only when the FTC sends "identical" questions to ten or more companies (whether their answer is voluntary or compulsory). The PRA would *not* apply to the FTC requesting public comment, such as it has done through the Green Guides process. This point is critical: while targeting specific companies with the same questions might well prove useful in informing the FTC's understanding of informational injuries, the FTC's failure to collect more such data thus far, to analyze it, and to publish it in useful guidance can in no way be blamed on the requirements of the PRA. Nor can it excuse the FTC staff for relying on an expert witness in the LabMD case whose recommendations about "reasonable" data security referred exclusively to the practices of Fortune 500 companies, without referencing *any* small businesses comparable in size and technical sophistication to LabMD.[194]

Indeed, the PRA Guide exempts from the definition of "information," and thus eliminates the need for clearance on, the collection of "facts or opinions submitted in response to general solicitations of comments from the general public"[195] and "examinations designed to test the

---

[192] *Id.*

[193] *See generally* Paperwork Reduction Act (PRA) Guide Version 2.0.

[194] Gus Hurwitz, *The FTC's Data Security Error: Treating Small Businesses Like the Fortune 1000* (Feb. 20, 2017), *available at* https://www.forbes.com/sites/washingtonbytes/2017/02/20/the-ftcs-data-security-error-treating-small-businesses-like-the-fortune-1000/#58d2b735a825.

[195] United States Office of Personnel Management, Paperwork Reduction Act (PRA), Version 2.0, OPM at 6 (April 2011), *available at* https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

aptitude, abilities, or knowledge of the person tested for a collection."[196] The PRA poses no impediment to the FTC taking a proactive approach on conducting empirical research on data privacy by calling for consumer survey participants, holding public workshops, or from analyzing public data such as companies' privacy policies as a means to test privacy risk perception and consumer expectations. The Green Guides illustrate just how much data collection the FTC can do to substantiate its policymaking with empirical and economic research, based on real consumer studies.

VIII. Pleading, Settlement and Merits Standards under Section 5

In general, the FTC Act currently sets a very low bar for bringing complaints: "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[197] In practice, this has become the standard for *settlements*, since the Act does not provide such a standard, and the FTC commonly issues both together. This raises three questions:

1. What should the standard be for issuing complaints?
2. Closely related, what should the standard be for courts weighing a defendant's motions to dismiss?
3. What should the standard be for settling cases?

Raising all three bars would do much to improve the quality of the agency's "common law" in several respects:

1. It would provide greater rigor for FTC staff throughout the course of the investigation;
2. Companies would be less likely to settle, and more likely to litigate, if they had a better chance of prevailing at the motion to dismiss stage; and
3. Complaints that settle before trial (after the FTC has survived a motion to dismiss) would, or complaints that the FTC has withdrawn (after the FTC has lost a motion to dismiss) would provide more guidance standing on their own as the final, principle record of each case.

We take the questions raised above in reverse order, beginning with the standard by which a court will assess a motion to dismiss and concluding with the standard by which Commissioners will decide whether to issue a complaint (and thus, in nearly every case, also a settlement):

[196] *Id*.

[197] 15 U.S.C. 45(b).

A. Pleading & Complaint Standards

Fortunately, the courts are already moving towards requiring the FTC to do a better job of writing its pleadings (complaints) or face dismissal of its complaints — at least with respect to deception. Congress should take note of the current case law on this issue and consider codifying a heightened pleading requirement for any use of Section 5.

Heightened pleading standards can be fatal to normal plaintiffs, who need to survive a motion to dismiss in order to obtain the discovery they need to actually prevail on the merits. But the FTC has uniquely broad investigative powers. It is difficult to see why they would *ever* need court-ordered discovery — in other words, why would it be a problem for the Commission to have to do more to ground their complaints in the requirements of Section 5, as made clear in the FTC's Deception and Unfairness policy statements, and Section 5(n). Today, the FTC wants the best of both worlds: vast pre-trial discovery power *and* the low bar for pleadings claimed by normal plaintiffs who lack that power.

At a minimum, the FTC should be required to plead its Section 5 claims with specificity. Ideally, this standard would closely mirror a "preponderance of the evidence," as explained in the attached white paper.[198]

1. Deception Cases

TechFreedom has long argued that the FTC's deception complaints should have to satisfy the heightened pleading standards of Fed. R. Civ. Pro. 9(b).[199] Under that rule, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."[200] In other words, such claims must be accompanied by the "who, what, when, where, and how" of the conduct charged.[201] Rule 9(b) gives defendants "notice of the claims against them, provide[ ] an increased measure of protection for their reputations, and reduce[ ] the number of frivolous suits brought solely to extract settlements."[202]

Several district courts have concluded that 9(b) applies to FTC deception allegations.[203] Most recently, the Northern District of California dismissed two of the FTC's five deception counts

---

[198] *See* White Paper, *supra* note 51, at 18-21 (unfairness) and 28 (deception).

[199] *See* Brief of Amicus Curiae TechFreedom, International Center for Law and Economics, & Consumer Protection Scholars in Support of Defendants, *FTC. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887), 2013 WL 3739729, *available at* https://goo.gl/JGUE9e.

[200] Fed. R. Civ. P. 9(b).

[201] *Vess v. Ciba–Geigy Corp., USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

[202] In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1418 (3d Cir. 1997).

[203] *See, e.g.,* FTC v. Lights of Am., Inc., 760 F. Supp. 2d 848 (C.D. Cal. 2010); FTC v. Ivy Capital, Inc., 2011 WL 2118626 (D. Nev. May 25, 2011); FTC v. ELH Consulting, LLC, No. CV 12-02246-PHX-FJM, 2013 WL 4759267,

in its data security complaint against D-Link[204] for failure to satisfy the heightened pleading standard of Rule 9(b).[205] The district court noted that the Ninth Circuit has yet to address the question, but nonetheless found controlling the appeals court's decision holding that California's Unfair Competition Law — the state's "Baby FTC Act," which, "like Section 5 outlaws deceptive practices without requiring fraud as an essential element" — is subject to Rule 9(b).[206]

The *D-Link* court's analysis of each of the FTC's five deception counts illustrates that, while a heightened pleading standard *would* require more work from Commission staff to establish their cases, this burden would be relatively small and would in no way hamstring the Commission from bringing legitimate cases. The court upheld the principal deception count (Count II: "that DLS has misrepresented the data security and protections its devices provide") and two others, dismissing only two peripheral claims. If anything, merely applying Section 9(b) to the Commission's complaints would likely not be enough, on its own, to provide adequate discipline to the Commission's use of its investigation and enforcement powers — but it would certainly be a start.

The district court's discussion of Count II illustrates what specificity in pleading deception claims would look like. The FTC's allegations identified "specific statements DLS made at specific times between December 2013 and September 2015," and that the allegations "also specify why the statements are deceptive."[207] The court goes on to say that "Count II identifies the time period during which DLS made the statements and provides specific reasons why the statements were false—for example, that the routers and IP cameras could be hacked through hard-coded user credentials or command injection flaws," and that "this is all Rule 9(b) demands."[208]

---

at *1 (D. Ariz. Sept. 4, 2013) (same); *see also* FTC v. Swish Marketing, No. C-09- 03814-RS, 2010 WL 653486, at *2-4 (N.D. Cal. Feb. 22, 2010) (finding "a real prospect" that Rule 9(b) applies but not deciding the issue).

[204] *See* Complaint for Permanent Injunction and Other Equitable Relief, *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), https://www.ftc.gov/system/files/documents/cases/d-link_complaint_for_permanent_injunction_and_other_equitable_relief_unredacted_version_seal_lifted_-_3-20-17.pdf.

[205] *See* Order Re Motion to Dismiss, *Fed. Trade Comm'n v. D-Link Sys.,* No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), *at* 2-3, https://consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf.

[206] *Id.* at 2-3 (discussing Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1103-04 (9th Cir. 2003)).

[207] *Id.* at 4.

[208] *Id.* at 4-5.

2. Unfairness Cases

The *D-Link* court noted that "[w]hether the FTC must also plead its unfairness claim under Rule 9(b) is more debatable," finding "little flavor of fraud in the[] elements [of unfairness under Section 5(n)]." But, the court continued:

> the FTC has expressly stated that the unfairness claim against DLS is not tied to an alleged misrepresentation. See Section III, below. At the same time, however, the FTC has said that for all of its claims "the core facts overlap, absolutely," and there is no doubt that the overall theme of the complaint is that DLS misled consumers about the data security its products provide. The FTC also acknowledges that DLS's misrepresentations are relevant to the unfairness claim because consumers could not have reasonably avoided injury in light of them.
>
> Consequently, there is a distinct possibility that Rule 9(b) might apply to the unfairness claim. But the question presently is not ripe for resolution. As discussed below, the unfairness claim is dismissed under Rule 8. Whether it will need to satisfy Rule 9(b) will depend on how the unfairness claim is stated, if the FTC chooses to amend.[209]

Whatever the courts actually conclude about the applicability of Rule 9(b) to unfairness claims, we see no reason why the Commission should not be subject to the same heightened pleading requirements under unfairness.

B. Preponderance of the Evidence Standard

Applying Section 9(b) to all Section 5 pleadings would help greatly. But the more fundamental problem in unfairness cases is the low bar set by Section 5(b) for bringing a complaint — and the lack of *any* standard for settling it. We believe the answer is to require the Commission staff to demonstrate that it would prevail by a preponderance of the evidence. It may, at first, seem strange to apply this standard — the general standard for resolving civil litigation — at the early stages of litigation, but it must be remembered that this is not normal litigation. As noted above, the FTC has unique pre-trial discovery powers, and so is very likely to have accumulated all the evidence it will need at trial before the complaint is ever issued. Second, in nearly every "informational injury" case, the Commission's decision over whether to issue a complaint *is* the final decision over the case — because the cause will simply settle at that point. Congress should consider applying this standard either to the issuance of unfairness complaints, or to the issuance of settlements. If the standard is applied only to the issuance of settlements, Congress should consider some other heightened standard for

[209] *Fed. Trade Comm'n v. D-Link Sys.,* at *2 (N.D. Cal. Sept. 19, 2017).

bringing unfairness complaints, above that required by Section 9(b). In any event, the purpose of any standard imposed at this stage would not be to change how litigation would work — which would still be resolved under separate standards for motions to dismiss, motions for summary judgment and final resolution of litigation on the merits — but rather to spur Commissioners to demand more analytical work of the staff. Some such change is likely the only way to create sustainable analytical discipline inside the Commission.

IX. Conclusion

There is little reason to expect that the FTC will not continue to more and more closely resemble the Federal Technology Commission with each passing year: the Commission will continue to grapple with new issues. This is just as Congress intended. But if the agency is to be trusted with such broad power, Congress should expect — and indeed take steps to ensure — that the FTC does more to justify how it wields that power. As Sens. Barry Goldwater (R-AZ) & Harrison Schmitt (D-AZ) said in 1980:

> Considering that rules of the Commission may apply to any act or practice "affecting commerce", and that the only statutory restraint is that it be unfair, the apparent power of the Commission with respect to commercial law is virtually as broad as the Congress itself. In fact, the Federal Trade Commission may be the second most powerful legislature in the country…. All 50 State legislatures and State Supreme Courts can agree that a particular act is fair and lawful, but the five-man appointed FTC can overrule them all. The Congress has little control over the far-flung activities of this agency short of passing entirely new legislation.[210]

This testimony, and the attached documents, lay out some of the ideas that Congress should consider in assessing how to reform the FTC's processes and standards. But these questions are sufficiently complex, and have been simmering for long enough, that the Committee would benefit from finding ways to maximize the input of outside experts.

One model for that would be the House Energy & Commerce Committee's ongoing #CommActUpdate effort.[211] The Committee has issued six white papers, each time taking public comment and refining its proposals. Given the complex interrelationships among the pieces of FTC reform, this would be a more constructive approach than having a flurry of separate bills, as Energy & Commerce did with FTC reform.

---

[210] S. Rep. No. 96-184, at 18 (1980), available at http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=417102.

[211] The Energy and Commerce Committee, #COMMSUPDATE (last visited Sept. 25, 11:00 AM), https://energycommerce.house.gov/commactupdate/.

The Committee could also consider establishing a blue-ribbon Commission modeled on the Antitrust Modernization Commission — as TechFreedom and the International Center for Law & Economics proposed in 2014:

> A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.[212]

We stand ready to assist the Committee in whatever approach it takes.

[212] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf

Testimony of

TechFreedom

Berin Szóka[1] & Graham Owens[2]

FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare

Hearing before the Subcommittee on Consumer Protection, Product Safety, Insurance, & Data Security of the U.S. Senate Committee on Commerce, Science, & Transportation

Tuesday, September 26, 2017

2:30 p.m.

Russell Senate Office Building
Room 253

---

[1] Berin Szóka is President of TechFreedom, a nonprofit, *nonpartisan* technology policy think tank. J.D. University of Virginia School of Law; B.A. Duke University. He can be reached at bszoka@techfreedom.org. With thanks to my dedicated legal staff at TechFreedom, and in particular Vinny Sidhu and Sunny Seon Kang.

[2] I. Graham Owens is a Legal Fellow with TechFreedom. J.D. George Washington University School of Law; B.A. University of Virginia. He can be reached at gowens@techfreedom.org.

Table of Contents

I. Introduction

Over the last two decades, use of, and access to, the Internet has grown exponentially, connecting people and businesses and improving the human condition in ways never before imagined. In 2011, 71.7% of households reported accessing the Internet, a sharp increase from 18 percent in 1997 and 54.7% in 2003.[3] This digital growth — from a network of computers that only a few consumers could reach, to a seemingly infinite marketplace of ideas accessible by almost all Americans — has benefited society beyond measure, affording consumers the ability to access information, purchase goods and services, and interact with each other almost instantaneously without having to leave the home.[4]

However, as use and benefits of the Internet has grown, so too has the collection of personal data and, consequently, cyber-attacks endeavoring to steal that data. Since 2013, the number of companies facing data breaches has steadily increased.[5] In 2016, 52% of companies reported experiencing a breach — an increase from 49% in 2015 — with 66% of those who experienced a breach reporting multiple breaches.[6] Perhaps not surprisingly, not much has changed since 2000, where one report revealed that system penetration by outsiders grew by 30% from 1998 to 1999.[7] Interestingly, despite immense improvements in companies' ability to anticipate and prevent cyber-attacks, some of the largest and most sophisticated companies in the world, including Sony, Target, eBay, and JPMorgan, continue to experience data breaches today,[8] just as they did in 2000.[9] In spite of these statistics, the United States currently has no comprehensive legal framework in which to inform companies of the best

---

[3] THOM FILE, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES 1 (May 2013), https://www.census.gov/prod/2013pubs/p20-569.pdf; *see also* Steve Case, The Complete History of the Internet's Boom, Bust, Boom Cycle, Business Insider (Jan. 14, 2011), *available at* http://www.businessinsider.com/what-factors-led-to-the-bursting-of-the-internet-bubble-of-the-late-90s-2011-1.

[4] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 1 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[5] PONEMON INST. LLC, FOURTH ANNUAL STUDY: IS YOUR COMPANY READY FOR A BIG DATA BREACH? 1 (2016), http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-preparedness-study.pdf [hereinafter PONEMON, DATA BREACH].

[6] *Id.*

[7] Hope Hamashige, *Cybercrime can kill venture*, CNN (March 10, 2000), http://cnnfn.cnn.com/2000/03/10/electronic/q_crime/index.htm (reporting the findings of the Computer Security Institute at Carnegie Mellon University).

[8] PONEMON INST. LLC, 2014: A YEAR OF MEGA BREACHES 1 (2015), http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

[9] Hamashige, *Cybercrime* (noting that, just as today, in 2000, "[e]ven the biggest Internet companies with the most sophisticated technology are vulnerable to hackers, a trend highlighted last month when hackers stopped traffic on several popular Internet sites including Yahoo!, Amazon.com and eBay.").

practices to both prevent or respond to cyber-attacks, as well as to ensure that they're acting responsibly in the eyes of the Government.[10]

Absent a comprehensive statutory framework, the Federal Trade Commission ("FTC" or "Commission") happily stepped in to police the vast number of data security and privacy practices not covered by the few Internet privacy and cyber security statutes enacted at the time. For two decades, the FTC has grappled with the consumer protection issues raised by the Digital Revolution. Armed with vast jurisdiction and broad discretion to decide what is unfair and deceptive, the agency has dealt with everything from privacy to data security, from online purchases to child protection, and much more. The FTC has become the Federal *Technology* Commission — a term we coined,[11] but which the FTC and others have embraced.[12]

This was inevitable, given the nature of the FTC's authority. Enforcing the promises made by tech companies to consumers forms a natural baseline for digital consumer protection. On top of that deception power, the FTC has broad power to police other practices, without waiting for Congress to catch up. As the FTC said in its 1980 Unfairness Policy statement:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion.[13]

---

[10] *See, e.g.,* ALAN CHARLES RAUL, TASHA D MANORANJAN & VIVEK MOHAN, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268 (Alan Charles Raul, 1st ed. 2014) ("With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather, allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin, 'unfair or deceptive' business practices.").

[11] Berin Szóka & Geoffrey Manne, The Second Century of the Federal Trade Commission, TECHDIRT (Sept. 26, 2013), available at https://www.techdirt.com/blog/innovation/articles/20130926/16542624670/secondcentury-federal-trade-commission.shtml; see also Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission, Report 1.0 of the FTC: Technology & Reform Project, 3 (Dec. 2013), available at http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[12] Kai Ryssdal, The FTC is Dealing with More High Tech Issues, MARKETPLACE (Mar. 7, 2016) (quoting then-Chairman Edith Ramirez), available at http://www.marketplace.org/2016/03/07/tech/ftc-dealing-more-high-tech-issues.

See, e.g., Omer Tene, *With Ramirez, FTC became the Federal Technology Commission*, IAPP (Jan. 18, 2017), https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/.

[13] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (hereinafter 1980 Unfairness Policy Statement).

The question is not whether the FTC *should* be the Federal Technology Commission, but *how* it wields its powers. For all that academics like to talk about creating a Federal Search Commission[14] or a Federal Robotics Commission,[15] and for all the talk in Washington of passing "comprehensive baseline privacy legislation" or data security legislation, the most important questions turn on the FTC's processes, standards, and institutional structure. How the FTC and Congress handle these seemingly banal matters could be even more important in determining how consumer protection works in 2117 than will any major legislative lurches over the next century. Indeed, with the costs of cybercrimes expected to reach $2 trillion by 2019,[16] the business community can ill afford to have to anticipate the approaches of both hackers and federal regulators simultaneously, and it would seem more practical for the agency to help guide businesses by providing best practices to better protect their consumers. Yet, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which do not admit liability and only focus on prospective requirements of the specific defendant in that case.[17]

This approach, and the resulting ambiguity, has left companies facing uncertainty in terms of whether their data security and privacy practices are not only sufficient to safeguard against an FTC enforcement action, but more importantly, whether they're utilizing the best practices available to protect their consumers' data and privacy.

---

[14] *See, e.g.,* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008), *available at* http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Bracha-Pasquale-Final.pdf.

[15] *See, e.g.,* Ryan Calo, *The case for a federal robotics commission*, Brookings Institute (Sept. 15, 2014), *available at* https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/; Nancy Scola, *Why the U.S. might just need a Federal Commission on Robotics*, Washington Post (Sept. 15, 2014), *available at* https://www.washingtonpost.com/news/the-switch/wp/2014/09/15/why-the-u-s-might-just-need-a-federal-commission-on-robots/?utm_term=.38dfc4bec72e.

[16] Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, Forbes (Jan. 17, 2016), *available at* https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6e10063a3a91.

[17] *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257, n.22. (3d Cir. 2015). Notably, this practice is not entirely limited to data security and privacy enforcement — though for reasons later discussed, the effects on companies are arguably more severe in this context — by the Commission, with one study finding that 1,524 of the 2,092 enforcement action brought by the FTC in either federal or administrative courts have ended in consent decrees without any adjudication. This means that almost 73% of the FTC's enforcement actions have ended in legally enforceable orders, despite no impartial judicial guidance as to the factual and legal legitimacy of the FTC's claims. *See* Daniel A. Crane, *Debunking Humphrey's Executor*, 83 GEO. WASH. L. REV. 1835, 1867 (2015). But in tech-related cases its almost 100%, meaning the courts have played essentially no role at all in disciplining the FTC's use of unfairness in "informational injury" cases. *See infra* note 122 (providing list of a few cases that did not result in settlement).

Understandably, this ambiguity has frustrated judges and legal commentators alike, even resulting in one company's demise. Such frustration was made abundantly clear by the Third Circuit when, despite affirming the FTC's authority to regulate cyber security practices under the "unfair practices" prong of Section 5, the court nonetheless questioned the Commission's assertion that its consent decrees and "guidance" somehow create standards against which companies' cyber practices can be tested for "unfairness."[18] In fact, the Third Circuit emphatically agreed with the defendant's claim that "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a)."[19] The court continued:

> We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." Oral Arg. Tr. at 51. We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples. *Id.* at 52.[20]

The court's frustration did not end with the Commission's use of consent decrees either, making sure to also address issues with the FTC's 2007 guidebook, *Protecting Personal Information, A Guide for Businesses*, which, according the FCC, "describes a 'checklist[]' of practices that form a 'sound data security plan.'"[21] Ultimately, the court recognized that "[t]he guidebook does not state that any particular practice is required by [Section 5]," and "[f]or this reason, we agree … that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[22]

Despite being rebuked by practitioners and courts alike, the FTC has brushed aside this frustration and continued to rely on consent decrees, conclusory guidebooks/reports, and "blog posts" to inform businesses as to what constitutes reasonable data security and privacy practices. By contrast, the FTC has pursued a radically different course, providing significantly more thorough guidance in an area not considered to be the FTC's primary jurisdiction — environmental regulations through "Green Guides." As explained below, these Green Guides

---

[18] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 252-253, 255 (3d Cir. 2015).

[19] *Id.* at 257 n.22.

[20] *Id.* at 257 n.23.

[21] *Id.* at 257.

[22] *Id.* at 257 n.21.

reflect a sincere and thoughtful effort by the FTC to gather relevant data as the basis for analyzing not only "what" is required, but more significantly "why" is it essential and "how much" of a certain practice is necessary.

On privacy and data security, the Commission has refused to do such empirical work or to issue clear guidance, relying instead on consent decrees and conclusory reports and guidebooks that lack any evident empirical foundation. This has deprived businesses of the regulatory certainty and clarity they need to comply with the law — and deprived consumers of better, more consistent data security and privacy practices. The Commission has flaunted the warning given it by the D.C. Circuit over forty years ago, that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible.[23] Ironically, the D.C. Circuit made that statement in a case where the FTC fought vehemently — and the court agreed — for the authority to provide the very guidance they refuse to provide to the digital economy today. Congress *did* provide that rulemaking authority a year later, with the Magnuson-Moss Act of 1975,[24] but also found it necessary to institute new procedural safeguards in 1980, after the FTC's gross abuse of its rulemaking powers in the intervening five years,[25] which culminated in the agency being denounced as the "National Nanny."[26]

With this backdrop in mind, I come before this Committee today with two goals. First, to inform this body — through a historical lens — of the FTC's ongoing procedural issues, particularly as they pertain to data security and privacy practices. Second, to use that historical analysis as a framework with which to propose practical process reforms that will ensure American businesses and the FTC work together as partners, not enemies, to make certain that consumers'—including Americans as well as foreign consumers who patronize U.S. businesses—data and privacy are afforded the greatest respect and protection possible.

---

[23] *Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974).

[24] The Magnuson-Moss Warranty Federal Trade Commission Improvement (Magnuson-Moss) Act, Pub.L.No. 93-637, § 202(a), 88 Stat. 2193 (1975).

[25] The Federal Trade Commission Improvements Act of 1980 (Improvements Act), Pub.L. No. 96-252, 94 Stat. 374 (1980).

[26] Editorial, WASH. POST (Mar. 1, 1978), reprinted in MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION, 69–70 (1982); *see also* J. Howard Beales III, *Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present*, 8 n.37 (2004), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kidsand-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf. ("Former FTC Chairman Pertschuk characterizes the Post editorial as a turning point in the Federal Trade Commission's fortunes.").

To that end, we herein provide a more in-depth historical analysis of the FTC's enforcement authority, including an examination of the problems that have arisen due to the FTC's current procedural issues. We detail how the FTC has utilized data-driven guidance in other contexts — namely the aforementioned Green Guides — to guide businesses through empirical analysis of available data. Finally, we use that historical context to frame ways that Congress can help urge the FTC to provide the same types of empirical guidance to the tech industry. Finally, I will discuss the underlying issues with the FTC's *very* low pleading standard and examine ways that Congress can address this problem.

Background of FTC Enforcement in the Digital Economy

While the FTC began studying online privacy issues as early as 1995,[27] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[28] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[29] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[30] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[31] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought

---

[27] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (June 1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter 1998 FTC Privacy Report] ("In April 1995, staff held its first public workshop on Privacy on the Internet, and in November of that year, the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues."); *see also* FED. TRADE COMM'N, A REPORT FROM THE FEDERAL TRADE COMMISSION STAFF: THE FTC'S FIRST FIVE YEARS PROTECTING CONSUMERS ONLINE (Dec. 1999), *available at* https://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-online/fiveyearreport.pdf.

[28] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[29] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[30] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[31] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[32] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[33] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[34] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[35]

In a speech last week, Acting Chairman Ohlhausen broadly summarized the "various types of consumer injury addressed in our privacy and data security cases" as "informational injury."[36] It's a useful shorthand: one term to describe a cluster of consumer protection problems behind a wide range of cases. But for the same reason, it's also a dangerous term — one that could, like "net neutrality," take on a life its own, and serve to obscure and frustrate analysis rather than inform it.[37] Of course, Chairman Ohlhausen chose her words carefully:

> [L]et me also emphasize that this is not a discussion of the legal question of what constitutes a 'substantial injury' under our unfairness standard. My topic today

---

[32] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[33] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[34] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[35] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[36] Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Painting the Privacy Landscape: Information Injury in FTC Privacy and Data Security Cases, Address Before the Federal Communications Bar Association (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf [hereinafter Ohlhausen, *Informational Injury Speech*].

[37] Larry Downes, *The Tangled Web of Net Neutrality and Regulation*, Harvard Business Review (March 31, 2017), *available at* https://hbr.org/2017/03/the-tangled-web-of-net-neutrality-and-regulation ("Despite being a simple idea, net neutrality has proven difficult to translate into U.S. policy. It sits uncomfortably at the intersection of highly technical internet architecture and equally complex principles of administrative law. Even the term "net neutrality" was coined not by an engineer but by a legal academic, in 2003."). Gerard Stegmaier, a veteran attorney in the field of data security and privacy, explained it as such: "Words matter. Net Neutrality. Deep Packet Inspection. #Privacy. Businesses beware. There's a new label in town from the gov't and repeating it could have significant unintended consequences. From a speech yesterday the @FTC acting chair declared "informational injuries" exist. Let that sink in." Posting of Gerard Stegmaier on LinkedIn.com (Sept. 20, 2017), *available at* https://www.linkedin.com/feed/update/urn:li:activity:6316291846356115456 (also on file with author).

> may inform the substantial injury question, but I am speaking more broadly. Indeed, many of the cases I will mention are deception cases, or allege both deception and unfairness.
>
> …
>
> In my review of our privacy and data security cases, I have identified at least five different types of consumer informational injury. Certain of these types are more common. Many of our cases involve multiple types of injury. Courts and FTC cases often emphasize *measurable* injuries from privacy and data security incidents, although other injuries may be present. And to be clear, not all of these types of injury, standing alone, would be sufficient to trigger liability under the FTC Act. [38]

It is fitting that she should emphasize the word "measurable" — and also caveat it with the word "often" — because both speak to the central question facing the Federal Technology Commission as it grapples with an endless, and accelerating, parade of novel consumer protection issues: *how* does the agency determine what the right answer is in any particular case and what should be done about it? Ohlhausen defended the FTC's approach to privacy and data security enforcement:

> Case-by-case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. As such, each case integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury.[39]

Yes, the courts' "feedback" is "important." Indeed, in a reply brief the FTC expressly agreed with TechFreedom on this importance of courts' guidance when it said it "agrees that the field would be aided by a body of law that includes 'Article III court decisions.'"[40] Yet, such assertions of the importance of courts' "feedback" by the FTC seem empty given there has been precious little of it. Since 1997, not counting a handful of cases where the FTC sought

[38] Ohlhausen, *Informational Injury Speech*, *supra* note 36, at 2-3.

[39] Ohlhausen, Informational Injury Speech, supra note 36, at 2.

[40] Plaintiff's Response In Opposition to the Motion to Dismiss, F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015) (No. 2:13-CV-01887-ES-SCM) at 22, n. 8.

injunctive relief against absent defendants (generally foreign scammers), the FTC has litigated, even partially, only a handful of cases: *LabMD*,[41] *Wyndham Worldwide Corp.*,[42] *Amazon.com, Inc.*,[43] and *D-Link Systems, Inc.*[44] Thus, the way the FTC works today is a far cry from what the FTC said about how it would operate back in 1980:

> The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[45]

What former FTC Chairman Tim Muris said of the Commission in 1981 remains true today: "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[46] As he noted in his 2010 testimony before a Senate Subcommittee, "the Commission's authority remains extremely broad."[47] What Commissioner Wright said of the FTC's competition enforcement — where the Commission differs from the DOJ in enforcing (in theory, anyway) the same substantive laws — is even more true of consumer protection:

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may

---

[41] LabMD, Inc. v. F.T.C., No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015).

[42] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[43] *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[44] *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017).

[45] 1980 Unfairness Policy Statement, *supra* note 12 (quoting *FTC v. Raladam Co.*, 283 U.S. 643, 648 (1931)).

[46] Timothy J. Muris, Judicial Constraints, in THE FEDERAL TRADE COMMISSION SINCE 1970: ECONOMIC REGULATION AND BUREAUCRATIC BEHAVIOR, 35, 49 (Kenneth W. Clarkson & Timothy J. Muris, eds., 1981).

[47] *Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. 2 (2010) (statement of Timothy J. Muris, Former Chairman, Fed. Trade Comm'n) *available at* http://lawprofessors.typepad.com/files/muris_senate_testimony_ftc_role_protecting_consumers_3-17- 101.pdf.

> not [violate any law or regulation]. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's [Section 5] authority by encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority.[48]

Without the courts to demand rigor from the FTC in defining "measurable" harm, what should the Commission do? And what should Congress do?

Chairman Ohlhausen's speech represents a major step in the right direction — precisely because it promises to give more analytical rigor to the term "informational injury" than such generalizations generally have. She concludes:

> This analysis raises several important questions. Is this list of injuries representative? When do these or other informational injuries require government intervention? Perhaps most importantly, how does this list map to our statutory deception and unfairness authorities?
>
> These are critical and challenging questions. That's why I am announcing today that the FTC will host a workshop on informational injury on December 12 of this year. This workshop will bring stakeholders together to discuss these issues in depth. I have three goals for this workshop: First, better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents. Second, explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence. And third, better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information. Ultimately, the goal is to inform our case selection and enforcement choices going forward.[49]

Amen. This is the kind of workshop the FTC should have held two decades ago — and several more times since. The FTC has, in fact, conducted such workshops, collected empirical data,

---

[48] Joshua D. Wright, *Revisiting Antitrust Institutions: The Case for Guidelines to Recalibrate the Federal Trade Commission's Section 5 Unfair Methods of Competition Authority*, 4 CONCURRENCES: COMPETITION L.J. 1 at 3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/siting-antitrust-institutions-case-guidelines-recalibrate-federal-trade-commissions-section-5-unfair/concurrences-4-2013.pdf.

[49] Ohlhausen, *Informational Injury Speech*, *supra* note 36 , at 9.

and issued corresponding guidance based upon rigorous empirical analysis in another context: the Green Guides first issued for environmental marketing in 1992, and updated three times since then.[50] As discussed below, these offer an excellent model for how the Commission could begin to take a more substantive approach to defining informational injury, while also providing clearer guidance to industry.

Congress should support and encourage this effort — by holding the FTC to the high standards set by its work on the Green Guides. If this effort represents a significant departure with the analytically flimsy, "know-it-when-we-see-it" approach the FTC has generally taken to "informational injury" cases thus far, both consumers and companies would benefit from clearer, better substantiated guidance. But this will not be an easy change to make; it will require a new degree of rigor in how the Bureau of Consumer Protection operates, and a new closeness in BCP's engagement with the Bureau of Economics.

At best, this could be the beginnings of a "law and economics" revolution in consumer protection law — of the sort that transformed competition law in decades past, has guided the Bureau of Competition since, and has informed the courts in their development of antitrust case law.

But at worst, this process could result in blessing the FTC's current approach with a veneer of analytical rigor that merely validates the status quo. The report that comes out of this process *could* resemble the reports the FTC has produced since the 2012 Privacy Report, which make broad recommendations as to what industry best practices should be, without any real analysis behind those recommendations or how they relate to the Commission's powers under Section 5.[51]

Chairman Ohlhausen's initial thoughtful framing suggests reason for optimism, but everything will depend on how she and whoever becomes permanent Chairman (if it is not her) execute on the plan. In any event, the Commission's own more recent experience with the

---

[50] *See* Fed. Trade Comm'n, *Environmental Friendly Products: FTC's Green Guides* (last visited Sept. 24, 2017), available at https://www.ftc.gov/news-events/media-resources/truth-advertising/green-guides ("The Green Guides were first issued in 1992 and were revised in 1996, 1998, and 2012. The guidance they provide includes: 1) general principles that apply to all environmental marketing claims; 2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and 3) how marketers can qualify their claims to avoid deceiving consumers.").

[51] *See* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE 57-60 (2016), *available at* http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf [hereinafter White Paper].

Green Guides — to say nothing of the last 15 years of experience with data security and privacy — suggests that self-restraint is unlikely to prove sustainable, on its own, in disciplining the agency. Ultimately, the kind of analytical quality that has defined antitrust law, and has sustained the law and economics approach there, requires *external* constraints — namely, regular engagement with the courts and oversight by Congress.

To that end, a careful reassessment of the Commission's processes is long overdue. The last time Congress seriously reconsidered, and revised, the FTC's processes was in 1994.[52] The agency has not been reauthorized since 1996.[53] Congress should return to its habit — the default assumption prior to Ken Starr, Monica Lewinsky, and impeachment — of reauthorizing the FTC every two years and, each time, re-examining how well the agency is working. Modifications to the statute should not be made lightly, but they should also happen more often than once in a generation.

Last year, the House Committee on Energy and Commerce considered no fewer than seventeen bills regarding the FTC. The attached white paper, co-authored with Geoffrey Manne, Executive Director of the International Center for Law & Economics, surveys those bills and provides recommendations to Congress on how to approach them.[54] Together, they form a starting point for the Senate Commerce Committee to begin its work, but they do not cover many of the most important aspects of how the agency works. Given this Committee's extensive knowledge and expertise, we hope that this Committee, along with the broader Senate, should start its own work on FTC reform legislation afresh.

II. Summary of Proposed Legislative Reforms

Rather than repeat the full analysis provided in the aforementioned white paper we presented to the House Energy & Commerce Committee last year, we have instead provided a short overview of how to consider thinking about the main issues we believe need to be addressed through legislation.

---

[52] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691 (Aug. 26, 1994) *available at* http://uscode.house.gov/statutes/pl/103/312.pdf.

[53] Federal Trade Commission Reauthorization Act of 1996, Pub. L. 104-216, 110 Stat. 3019 (Oct. 1, 1996), *available at* http://uscode.house.gov/statutes/pl/104/216.pdf.

[54] *See generally* White Paper, *supra* note 51.

A. The Common Carrier Exception

The FTC Act excludes "common carriers subject to the Acts to regulate commerce."[55] What this provision means will be crucial — especially for technology cases in the coming years — and merits clarification from Congress.

The Federal Communications Commission has proposed to undo its 2015 reclassification of broadband providers as common carriers.[56] Doing so will return the controversial issue of "net neutrality" to the Federal Trade Commission by restoring the FTC's jurisdiction over broadband providers — or rather, there *should* be a seamless transition to ensure that consumers remain protected. But a Ninth Circuit panel decision last year calls into question whether the FTC's jurisdiction will be fully restored,[57] creating the possibility that a company providing broadband service, once that service is no longer considered a common carrier service by the FCC, might still remain outside the jurisdiction of the FTC either because (1) that particular corporate entity also provides a common carrier service such as voice (which will remain subject to Title II of the Communications Act even after the FCC's proposes re-reclassification of broadband) or (2) another corporate entity under common ownership provides such a common carrier service. In short, the panel decision rejected the FTC's longstanding "activity-based" interpretation of the statute in favor of an "entity-based" interpretation. The Ninth Circuit granted rehearing of that decision earlier this year, effectively vacating the panel decision.[58]

At oral arguments last week, AT&T stuck by its general arguments for an entity-bases interpretation, but clarified two things.[59] First, it read the statute to turn on the common carrier or non-common carrier status of each specific corporate entity, so that the FTC's jurisdiction over Oath, for example, the company formed by the Verizon parent company after it acquired AOL and Yahoo! and merged them together, would not be affected by the fact that Verizon Wireless provides a common carrier voice service. Second, AT&T argued that the FCC has plenary jurisdiction to, as it did in the *Computer Inquiries*, mandate such structural separation to ensure that there is no gap in consumer protection between the FTC and FCC.[60]

---

[55] 15 U.S.C. § 45(a).

[56] Notice of Proposed Rulemaking, Restoring Internet Freedom, WC Docket No. 17-108, 32 FCC Rcd 4434 (2017), https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1_Rcd.pdf.

[57] *Fed. Trade Comm'n v. AT & T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), *reh'g en banc granted sub nom*., *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017).

[58] Fed. Trade Comm'n v. AT&T Mobility LLC, 864 F.3d 995 (9th Cir. 2017).

[59] United States Court of Appeals for the Ninth Circuit, *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (2017), Oral Arguments, *available at* https://www.youtube.com/watch?v=Rs8EQU-KIEw.

[60] *Id.* at 13:50.

It is impossible to predict how the Ninth Circuit might resolve this case, but it is safe to say that if the FCC issues its Third Open Internet Order this year, or even early next year, that decision might well come out before the Ninth Circuit's decision.

Congress should not assume that the Ninth Circuit will fully restore the FTC's activity-based interpretation of its jurisdiction, even though appears to be the most likely result of the case. Congress should, instead, consider quickly moving legislation that would codify that interpretation. Even if the Ninth Circuit en banc panel accepts AT&T's argument and simply narrows the panel decision, that would only solve part of the problem raised by the panel decision. Requiring structural separation between "edge" companies like Oath and broadband companies like Verizon *might* make business sense anyway, but it might not — especially given the ongoing push to restrict the sharing of consumer data *even among corporate affiliates under common ownership*. Furthermore, AT&T's argument would still raise serious questions about which agency will deal with net neutrality and other consumer protection concerns about broadband services once they are returned to Title I: it is difficult to see how the common carrier services provided by these companies, if only telephony, could be functionally separated from the broadband service. Would consumers have to deal with, and subscribe to, two separate services, each offered by a separate corporate entity?

The Ninth Circuit may, of course, reject AT&T's arguments completely, fully reverse the panel decision, and restore the FTC's activity-based interpretation completely. But it would be far better for Congress to resolve this question before the FCC revises the regulatory classification of broadband. It could do so in a one-sentence bill.

Of course, many have argued that the common carrier exception should be abolished, and the Protecting Consumers in Commerce Act of 2016 (H.R. 5239) would have done just that.[61] Simply restoring the activity-based exemption need not be permanent; it could be stop-gap measure that allows Congress time to consider whether to maintain the exemption.

B. More Economic Analysis

As many commentators have noted, the FTC has frequently failed to employ sufficient economic analysis in both its enforcement work and policymaking. Former Commissioner Josh Wright summarized the problem pointedly in a speech entitled "The FTC and Privacy Regulation: The Missing Role of Economics," explaining:

> An economic approach to privacy regulation is guided by the tradeoff between the consumer welfare benefits of these new and enhanced products and services

[61] Protecting Consumers in Commerce Act of 2016, H.R. 5239, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/5239/text.

> against the potential harm to consumers, both of which arise from the same free flow and exchange of data. Unfortunately, government regulators have instead been slow, and at times outright reluctant, to embrace the flow of data. What I saw during my time at the FTC is what appears to be a generalized apprehension about the collection and use of data – whether or not the data is actually personally identifiable or sensitive – along with a corresponding, and arguably crippling, fear about the possible misuse of such data.[62]

As Wright further noted, such an approach would take into account the risk of abuses that will cause consumer harm, weighed with as much precision as possible. Failing to do so can lead to significant problems, including creating disincentives for companies to innovate and create benefits for consumers.

Specifically, Congress or the FTC should require the Bureau of Economics to have a role in commenting on consent decrees[63] and proposed rulemaking,[64] and a greater role in the CID process. But the most effective ways to engage economists in the FTC's decisionmaking would be to raise the FTC's pleading standards and make reforms to the CID process designed to make litigation more likely: in both cases, the FTC will have to engage its economists more closely, either in order to ensure that its complaints are well-plead or to prevail on the merits in federal court.

C. Clarification of the FTC's Substantive Standards

The FTC has departed in significant ways from both the letter and spirit of the 1980 Unfairness Policy Statement and the 1983 Deception Policy Statement. This is mainly due to the FTC essentially having complete, unchecked, discretion to interpret these policy statements as it sees fit — including the discretion to change course regularly without notice. The courts simply have not had the opportunity to effectively implement Section 5(n), nor has the FTC ever really chosen to constrain its own discretion in meaningful ways (as it has done with the Green Guides). Making substantive clarifications to Section 5 will not be adequate without *process* reforms to ensure that these clarifications are given effect over time. But that does not mean they would be without value.

---

[62] Remarks of Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, George Mason University Law and Economics Center (Nov. 12, 2015), *available at* http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

[63] *See* White Paper, *supra* note 51, at 42-43.

[64] *See id*. at 98-100.

In order to clarify the FTC's substantive standards under Section 5, we would suggest the following key changes:

1. Codifying other key aspects of the 1980 Unfairness Policy Statement into Section 5 that were not already added by the addition of Section 5(n) in 1994;
2. Codifying the Deception Policy Statement, just as Congress codified the Unfairness Policy Statement in a new Section 5(n).[65] This issue is explored in greater depth in my 2015 joint comments with Geoffrey Manne on the FTC's settlement of its enforcement action with Nomi Technologies, Inc.[66] Specifically, in codifying the Deception Policy Statement, Congress should:
    a. Clarify — or require the FTC to propose clarifications of — when and how the FTC must establish the materiality of statements about products: it made sense to presume that all express statements were material in the context of traditional advertising: because each such statement was calculated to persuade users to buy a product. But the same cannot *necessarily* be said of the myriad other ways that companies communicate with users today, such as through online help pages or privacy policies (which companies are required to post online, if only by California law).
    b. Require the FTC to meet the requirements of Section 5(n) when bringing enforcement actions based on the "reasonableness" of a company's practices, such as data security.[67]
3. Codify the FTC's 2015 Unfair Methods of Competition Policy Statement, with one small modification: the FTC should be barred from going beyond antitrust doctrine.[68]

[65] *See* White Paper, *supra* note 51, at 21-28.

[66] *In the Matter of Nomi Technologies, Inc.*, Comments of the International Center for Law & Economics & TechFreedom, File No. 1323251 (May 26, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/05/00011-96185.pdf.

[67] *See infra* 69.

[68] *See* White Paper, *supra* note 51, at 28-30; Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

D. Clarifying the FTC's Pleading Standards

Several courts have already concluded that the FTC's deception enforcement actions must satisfy the heightened pleading standards of Section 9(b) of the Federal Rules of Civil Procedure, which applies to claims filed in federal court that "sound in fraud."[69] As explained below, this requirement would not be difficult for the FTC to meet, since the agency has broad Civil Investigative powers that are not available to normal plaintiffs before filing a complaint.[70] There is no reason the FTC should not have to plead its deception claims with specificity.

The same can be said for unfairness claims, even though they do not "sound in fraud." In both cases, getting the FTC to file more particularized complaints is critical, given that the FTC's complaint is, in essentially all cases, the FTC's last word on the matter, supplemented by little more than a press release, and an aid for public comment.

Indeed, the bar should likely be *higher*, not lower for unfairness cases. The attached white paper recommends a preponderance of objective standard for unfairness cases.[71] The critical thing to note is that there is no statutory standard for settling FTC enforcement actions — so the standard by which the FTC really operates is the very low bar set by Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[72] In addition to the substantive clarifications to the FTC's substantive standards, Congress must clarify either the settlement standard or the pleading standard, if not both.

E. Encouraging More Litigation to Engage the Courts in the Development of Section 5 Doctrine and Provide More Authoritative Guidance

Litigation is important for two reasons. First, having to prove its case before a neutral tribunal forces analytical rigor upon the FTC and thus forces it to make better, more informed decisions. Second, court decisions will provide guidance to regulated companies on how to comply with the law that is necessarily more authoritative (since the FTC cannot simply overrule a court decision the way it can change its mind about its own enforcement actions

---

[69] Rombach v. Chang, 355 F.3d 164, 170 (2d Cir. 2004) ("In deciding this issue, several circuits have distinguished between allegations of fraud and allegations of negligence, applying Rule 9(b) only to claims pleaded under Section 11 and Section 12(a)(2) that sound in fraud.").

[70] *See infra* at 19.

[71] *See* White Paper, *supra* note 51, at 18-21.

[72] 15 U.S.C. § 45(b).

or guidance) and also likely (but not necessarily) more detailed and better grounded in the FTC's doctrines.

One major reason companies settle so often across the board is that the FTC staff has the discretion to force companies to endure the process of litigating through the FTC's own administrative process, first before an administrative law judge and then before the Commission itself, before ever having the opportunity to go before an independent, neutral tribunal. The attached white paper explore three options:[73]

1. "[E]mpower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective."[74]
2. Abolish Part III completely, as former Commissioner Calvani has proposed.[75]
3. Require the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery.[76] Requiring the FTC to litigate all cases in federal court (as the SMARTER Act would do for competition cases[77]) might, in principle, prove problematic for the Bureau of Consumer Protection, which handles many smaller cases. Retaining Part III but allowing Commissioners to object to its use might strike the best balance.

F. The Civil Investigative Demand Process

There are many reasons why companies do not litigate privacy and data security cases. Some of them are beyond the control of FTC or Congress — for example, the extreme sensitivity of these issues for companies. Studies by the Ponemon Institute found that "[d]ata breaches are more concerning than product recalls and lawsuits,"[78] with a company's stock price falling

[73] *See* White Paper, *supra* note 51, at 82-85.

[74] *Id.*

[75] *See id*. at 84-85.

[76] *Id.*

[77] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015).

[78] PONEMON, DATA BREACH, *supra* note 5, at 6.

an average of 5% after a data breach is disclosed.[79] Witness the 30% hit Equifax took to its stock price upon revelation of its data breach.[80] Perhaps most illustrative of the sensitivity of these issues was the case of LabMD — a medical testing company and one of the handful of companies who dared litigate against the FTC — which ultimately went out of business due to litigation costs and reputational damage, even though the judge ultimately found that no consumer was injured.[81] But a very significant, if not the biggest, reason why companies reflexively, almost invariably settle their cases is that the process of the FTC's investigation can be punishment enough to make settlement seem more attractive. After enduring a burdensome investigative process, companies (especially start-ups) frequently lack additional resources to defend themselves and face an informational asymmetry given the intrusiveness inherent in the FTC's current process. Even Chris Hoofnagle, who has long advocated that the FTC be far more aggressive on privacy and data security, warns, in his new treatise on privacy regulation at the agency, that

> [T]he FTC's investigatory power is very broad and is akin to an inquisitorial body. On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[82]

This onerous the process inevitably leads to more false-positives as FTC staff becomes invested in fishing expeditions and force such consent decrees regardless of the actual harms on consumers.[83] Other systemic costs of this process include increased discovery burdens on (even blameless) potential defendants, inefficiently large compliance expenditures throughout the economy, under experimentation and innovation by firms, doctrinally questionable consent orders, and a relative scarcity of judicial review of Commission enforcement decisions. Ultimately, this phenomena distorts the FTC's consumer protection mission because the agency can self-select cases that are likely to settle and further its policy goals,

---

[79] *See* Help Net Security, *After a data breach is disclosed, stock prices fall an average of 5%* (May 16, 2017), https://www.helpnetsecurity.com/2017/05/16/data-breach-stock-price/ (detailing a study by Ponemon).

[80] Paul R. La Monica, *After Equifax apologizes, stock falls another 15%* (Sept. 13, 2017), *available at* http://money.cnn.com/2017/09/13/investing/equifax-stock-mark-warner-ftc-probe/index.html.

[81] *See, e.g.,* Cheryl Conner, *When The Government Closes Your Business*, Forbes (Feb. 1, 2014), https://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/#6e7c78971435; Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, Bloomberg (April 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/ ("The one company that didn't settle with the FTC is LabMD. Daugherty hoped, at first, that if he were as cooperative as possible, the FTC would go away. He now calls that phase 'the stupid zone.'").

[82] Darren Bush, The Incentive and Ability of the Federal Trade Commission to Investigate Real Estate Markets: An Exercise in Political Economy, 20-21, available at http://www.antitrustinstitute.org/files/517c.pdf.

[83] *See* Geoffrey A. Manne, R. Ben Sperry & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1 (2015).

rather than choosing cases on the basis of stopping the most nefarious actors and truly protecting consumers. As even former FTC Commissioner Joshua Wright noted, such self-serving personal and agency goals may push agencies to pursue cases "with the best prospect for settlement, cases that will consume few investigative resources, settle quickly, and are more likely to result in a consent decree that provides a continuing role for the agency."[84] Thus, more than any other aspect of the FTC Act or the FTC's operations, it is here that reinvigorated congressional oversight is needed.

The attached white paper explores this topic in great depth. Specifically, we recommend:

1. Reporting on how the agency uses CIDs[85]
2. Making CIDs confidential by default and allowing companies to move to quash them confidentially.[86] Today, fighting an FTC subpoena means the FTC can make the fight public, which may have serious consequences for a company's brand and stock price.
3. Requiring a greater role for Commissioners and economists in supervising the discovery process.[87]

Ultimately, any examination of the FTC's processes should start with arguably the most sacred principle in the American judicial system: innocent until proven guilty. As the Supreme Court made clear in 1895, "[t]he principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law."[88] While it is inarguably true that these cases are very clearly not criminal, it is also true that these companies and their employees face the threat of losing their "life, liberty, and property" as a result of these actions, as evidenced by LabMD. Despite the Administrative Law Judge finding that "the evidence fails to show any computer hack for purpose of committing identity fraud," the employees of LabMD were nonetheless left without employment simply due to "speculation" by the FTC — a word that appeared seventeen times in the ALJ's decision.[89]

Given the sensitive nature of both the type of information involved in these cases, including financial and health information, as well as consumers' sensitivity to reports that their data

---

[84] D.H. Ginsburg & J.D. Wright, *Antitrust Settlements: The Culture of Consent, in* I. William E. Kovacic: An Antitrust Tribute – Liber Amicorum (Charbit et al. eds., February 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/antitrust-settlements-culture-consent/130228antitruststlmt.pdf.

[85] *See* White Paper, *supra* note 51, at 37-40.

[86] *Id.* at 46-48.

[87] *Id.* at 48-53.

[88] *Coffin v. United States*, 156 U.S. 432, 453 (1895).

[89] LabMD, Inc., No. 9357, 2015 WL 7575033, at *48 (MSNET Nov. 13, 2015), https://causeofaction.org/wp-content/uploads/2015/11/Docket-9357-LabMD-Initial-Decison-electronic-version-pursuant-to-FTC-Rule-3-51c21.pdf.

may be in jeopardy, it is of the utmost importance that Congress ensure that innocent businesses' reputations aren't irreparably damaged simply due to "speculation." To be clear: this is not to say that parties who are guilty of implementing nefarious practices should be protected from the court of public opinion. Indeed, as former Commissioner Wright alluded to, implementing processes that would, at the very least, require the FTC to plead its claims with specificity — and, ideally, subsequently prove it on the basis of data-driven standards — prior to dragging a companies' name through the mud would actually ensure the FTC was using its limited resources to *only* go after the worst actors, rather than merely those most likely to settle.

Requiring the FTC to first make a showing beyond "speculation" of harm it alleges before invoking its immensely broad investigatory power, would at least provide businesses and its employees with some level of protection before being labeled as having unsecure data practices and being forced to face the repercussions that inevitably come with such a label. In doing so, Congress would ensure one of the oldest maxims of law in democratic civilizations continues. As Roman Emperor Julian eloquently quipped in response to his fiercest adversary's statement that "Oh, illustrious Caesar! if it is sufficient to deny, what hereafter will become of the guilty?": "If it suffices to accuse, what will become of the innocent?"[90]

G. Fencing-In Relief

The FTC has broad powers under Section 13(b) to include in consent decrees extraordinarily broad behavioral requirements that "fence in" the company in the future.[91] The courts have been exceedingly deferential to the FTC in applying these requirements, though at least one circuit court has rebuked the FTC's broad approach, as explained in the attached white paper.[92] Rather than attempting to limit how the FTC uses its 13(b) powers, Congress should focus on when Section 13(b) applies. As Howard Beales, former director of the Bureau of Consumer Protection, has argued, regarding deception:

> the Commission's use of Section 13(b) remedies should be reevaluated in light of the law's original purpose: [O]ne class of cases clearly improper for awarding redress under Section 13(b): traditional substantiation cases, which typically involve established businesses selling products with substantial value beyond the

[90] *Coffin v. United States*, 156 U.S. 432, 455 (1895).

[91] *See*, *e.g., Kraft, Inc. v. F.T.C.*, 970 F.2d 311, 326 (7th Cir. 1992) ("The F.T.C. has discretion to issue multi-product orders, so called 'fencing-in' orders, that extend beyond violations of the Act to prevent violators from engaging in similar deceptive practices in the future.") (citing *F.T.C. v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

[92] *See* White Paper, *supra* note 51, at 73-75.

> claims at issue and disputes over scientific details with well-regarded experts on both sides of the issue. In such cases, the defendant would not have known ex ante that its conduct was "dishonest or fraudulent." Limiting the availability of consumer redress under Section 13(b) to cases consistent with the Section 19 standard strikes the balance Congress thought necessary and ensures that the FTC's actions benefit those that it is their mission to protect: the general public.[93]

The same logic goes for the kind of unfairness cases the FTC is bringing against high-tech companies, as Josh Wright noted in his dissent in the *Apple* product design case:

> The economic consequences of the allegedly unfair act or practice in this case — a product design decision that benefits some consumers and harms others — also differ significantly from those in the Commission's previous unfairness cases. The Commission commonly brings unfairness cases alleging failure to obtain express informed consent. These cases invariably involve conduct where the defendant has intentionally obscured the fact that consumers would be billed. Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud — the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items. Under this scenario, the allegedly unfair act or practice injures consumers and does not provide economic value to consumers or competition. In such cases, the requirement to provide adequate disclosure itself does not cause significant harmful effects and can be satisfied at low cost. However, the particular facts of this case differ in several respects from the above scenario.[94]

The key point, as Wright argued, is that the Commission is increasingly using unfairness not to punish obviously bad actors or to proscribe conduct that merits *per se* illegality because it is inherently bad, but rather, conduct that presents difficult tradeoffs: How long should consumers remained logged in to an apps store to balance the convenience of the vast majority of users with the possibility that some users with children may find that their children make unauthorized purchases on the device immediately after the parent has logged in? How much, and what kind of, data security is "reasonable?" And so on. These reflect business decisions that are inevitable in the modern economy. The Commission might well be justified in declaring that a company has struck the wrong balance, but it should not treat them exactly as it would obvious fraudsters, who set out to defraud consumers.

---

[93] J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(b) of the FTC Act*, 79 ANTITRUST L. J. 1, 6-7 (2013).

[94] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 3 (Jan. 15, 2014), available at https://goo.gl/0RCC9E.

In order to deter the Commission from taking advantage of this frequent judicial deference by imposing such disconnected "fencing-in" remedies in non-fraud cases — which, of course, is compounded by the fact that most cases are never reviewed by courts at all — Congress should consider imposing some sort of minimal requirement that provisions in proposed orders and consent decrees be (i) reasonably related to challenged behavior, and (ii) no more onerous than necessary to correct or prevent the challenged violation.

H. Closing Letters

While consent decrees might help companies understand what the FTC will deem illegal on a case-by-case basis, in unique fact patterns, closing letters could do the inverse, telling companies what the FTC will deem *not* to be illegal, which is potentially far more useful in helping companies plan their conduct. In the past, the FTC issued at least a few closing letters with a meaningful degree of analysis of the practices at issue under the doctrinal framework of Section 5(n).[95] But in recent years, the FTC has markedly changes its approach, issuing fewer letters and writing those it did issue at a level of abstraction that offers little real guidance and even less analysis.[96]

Rep. Brett Guthrie's (R-KY) proposed CLEAR Act (H.R. 5109) would require the FTC to report annually to Congress on the status of its investigations, including the legal analysis supporting the FTC's decision to close some investigations without action. This requirement would not require the Commission to identify its targets, thus preserving the anonymity of the firms in question.[97] Most importantly, the bill requires:

> (1) IN GENERAL.—The Commission shall, on an annual basis, submit a report to Congress on investigations with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of subsection (a)(1)), detailing—
>
> > (A) the number of such investigations the Commission has commenced;
> >
> > (B) the number of such investigations the Commission has closed with no official agency action;

[95] *Id.* at 40-43. *See, e.g.,* Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf .

[96] *See, e.g*., Letter from Maneesha Mithal, Associate Director of Fed. Trade Comm'n to Lisa J. Sotto, Counsel to Michael's Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-storesinc./120706michaelsstorescltr.pdf.

[97] The Clarifying Legality and Enforcement Action Reasoning Act, H.R. 5109, 114th Cong. (2016) [hereinafter CLEAR Act] available at https://www.congress.gov/bill/114th-congress/house-bill/5109/text.

> (C) the disposition of such investigations, if such investigations have concluded and resulted in official agency action; and
>
> (D) for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal ***and economic*** analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

This bill, with our proposed addition noted, would go a long way to improving the value of the FTC's guidance. Indeed, such annual reporting could form annual addenda to guidance that the FTC issues in the guidance it provides on informational injury modeled on the Green Guides. Although the Green Guides themselves do not involve such reporting, it would make sense in this context, where the FTC is regularly confronted with far more novel fact patterns each year.

I. Re-opening Past Settlements

The FTC may, under its current rules, re-open past settlements at any time — subject only to the Commission's assertion about what the "public interest" requires and after giving companies an opportunity to "show cause" why their settlements should *not* be modified.[98] By contrast, courts require far more for re-opening their orders. The FTC has, in fact, proposed to re-open four settlements entered into in 2013 under the Green Guides. Congress should write a meaningful standard by which the FTC should have to justify re-opening past settlements. If the Commission continues on its current course, it will be able to use its settlements to bypass the procedural safeguards of notice-and-comment rulemaking.

III. Reasonable Siblings: Background on Section 5 and Negligence

The FTC's enforcement authority is derived from Section 5 of the Federal Trade Commission Act (FTC Act), which declares unlawful "[u]nfair methods of competition in or affecting commerce" and "unfair or deceptive acts or practices in or affecting commerce."[99] Under the broad terms of Section 5, the FTC challenges "unfair methods of competition" through their

[98] 16 C.F.R. 3.72(b).

[99] 15 U.S.C.A. § 45 (West 2017).

antitrust division and "unfair or deceptive practices" through their consumer protection division.[100] In pursuing its consumer protection mission there are different standards for "unfair" and "deceptive" practices, with its unfairness authority being "the broadest portion of the Commission's statutory authority."[101] Indeed, this "unfairness" authority was initially unrestrained by any statutory definition,[102] and remained so until Congress added Section 5(n) in 1994. In addition to Section 5 authority, however, the FTC has also asserted violations of other statutes in its data security enforcement, most notably the Gramm-Leach-Bliley Act ("GLBA"),[103] Children's Online Privacy Protection Act ("COPPA"),[104] as well as regulations promulgated under those statutes.[105]

Congress intentionally framed the FTC's authority under Section 5 in the general terms "unfair" and "deceptive" to ensure that the agency could protect consumers and competition throughout all trade and under changing circumstances.[106] To be sure, this broad authority has not been lost on the FTC, who readily acknowledges that "Congress intentionally framed the statute in general terms," which the agency interprets to mean "[t]he task of identifying unfair methods of competition" as being "assigned to the Commission."[107] Despite the addi-

---

[100] *See generally* Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law,* 101 Iowa L. Rev. 955, 964 (2016) (discussing in great lengths the FTC's "common law" approach) [hereinafter Hurwitz, *Uncommon Law*].

[101] *Id*.

[102] *See Id*.; *see also* Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) (setting the three-factor contours of the "unfairness" prong for the first time through application of Section 5 to cigarette advertisements).

[103] *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (2012) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to … protect the security and confidentiality of … customers' nonpublic personal information.").

[104] The Child Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, *et seq* (1994 & Supp. IV 1998) (making it unlawful under § 6502(a)(1) "for an operator of a website or online service directed to children … to collect personal information form a child in a manner that violates the regulations prescribed under subsection (b) of this section."); *see also* Melanie L. Hersh, Is Coppa A Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet, 28 Fordham Urb. L.J. 1831, 1878 (2001) (detailing how the FTC uses COPPA to regulate data security for children).

[105] *See, e.g.,* FTC Final Rule, 16 C.F.R. §§ 313.10–313.12 (2000); *Individual Reference Servs. Grp., Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 20 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. F.T.C.*, 295 F.3d 42 (D.C. Cir. 2002) (holding that the FTC's final rule, promulgated under the GLBA "did not contravene plain meaning of Act and were permissible construction of that legislation" and "agencies' action in promulgating final rules was not arbitrary and capricious").

[106] *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (observing if Congress "were to adopt the method of definition, it would undertake an endless task").

[107] Joshua D. Wright, Commissioner, Federal Trade Comm'n, Section 5 Recast: Defining the Federal Trade Commission's Unfair Methods of Competition Authority at the Executive Committee Meeting of the New York

tion of Section 5(n) to the Act in 1994 to *require* cost-benefit analysis, this lack of clear statutory guidance as to what constitutes "unfair" proved to be problematic, with at least one Commissioner recently recognizing that "nearly one hundred years after the agency's creation, the Commission has still not articulated what constitutes … unfair… leaving many wondering whether the Commission's Section 5 authority actually has any meaningful limits."[108] Commissioner Wright was referring to a lack of clarity around the meaning of unfairness in competition cases, but his point holds more generally.

Given the broad nature of Section 5, few industries are beyond the FTC's reach and the FTC has met the broad statutory language with an equally broad exercise of its authority to enforce Section 5.[109] The FTC has brought data security and privacy actions against advertising companies, financial institutions, health care companies, and, perhaps most significantly, companies engaged in providing data security products and services.[110] Further, not only are companies responsible for safeguarding their own data, but the FTC has also alleged that companies are responsible for any data security failings of their third-party clients and vendors, too.[111]

Companies who are the victims of such cyber-attacks are victims themselves. They suffer immense financial losses, stemming largely from reputational damage as customers are fearful of remaining loyal to companies who can't protect their personal and financial information.[112] According to one study, 76% of customers surveyed said they "would move away from companies with a high record of data breaches," with 90% responding that "there are

---

State Bar Association's Antitrust Section, 2 (June 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/section-5-recast-defining-federal-trade-commissions-unfair-methods-competition-authority/130619section5recast.pdf.

[108] *Id*.

[109] *See* Cho & Caplan, *Cybersecurity Lessons*; Stuart L. Pardau & Blake Edwards, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity 12 J. Bus. & Tech. L. 227, 232 (2017) (discussing the FTC's enforcement of "everything from funeral homes, vending machine companies, telemarketing and mail marketing schemes, credit reporting, and the healthcare industry.") [hereinafter Pardau & Edwards, *New Legal Frontiers*].

[110] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[111] *See id.* (For example, the consent decree agreed to in the FTC's enforcement action against Ashley Madison required the defendants to implement a comprehensive data-security program, including third-party assessments).

[112] *See generally* PONEMON, DATA BREACH; *see also Data breaches cost US businesses an average of $7 million – here's the breakdown*, Business Insider (April 27, 2017), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4 (providing that the average cost of a data security breach is $7 million, with 76% of customers saying they would move away from companies with a high record of data breaches).

apps and websites that pose risks to the protection and security of their personal information."[113] Unquestionably, data security is the cornerstone of the digital economy and digitization of the physical economy. As Naveen Menon, President of Cisco Systems for Southeast Asia, put it "[s]ecurity is what protects businesses, allowing them to innovate, build new products and services."[114]

The recent Equifax breach illustrates just how strongly reputational forces encourage companies to invest in data security. As of the time this testimony was being written, Equifax's post-hack stock had plummeted 30%.[115] Given the enormous stakes for companies' brands, it is not difficult to understand why—with no clear guidance from Congress or the FTC—companies have opted to settle and enter into consent decrees rather than risk further reputational damage and customer loss through embarrassing and costly litigation.[116] Out of approximately 60 data security enforcement actions, only two defendants dared face an FTC armed with near absolute discretion as to the interpretation of "reasonable" data security practices. This hesitation to challenge the FTC in order to gain clarity from the courts about what actually constitutes unreasonable practices — in addition to the more obvious reason of escaping liability — was only reinforced by the *LabMD* case, where the company's decision to litigate against the FTC rather than enter into a consent decree led to its demise.[117]

Data security poses a unique challenge: unlike other unfairness cases, the company at issue is both the victim (of data breaches) and the culprit (for allegedly having inadequate data security). In such circumstances, the FTC should apply unfairness as more of a negligence standard than strict liability. Consider both a company that has been hacked and a business owner whose business has burned down. In both situations, it is very likely that employees and customers lost items they consider to be precious — perhaps even irreplaceable. Additionally, it is equally likely that neither *wanted* this unfortunate event to occur. Finally, in both situations, prosecutors would investigate the accident to determine the cause and as-

---

[113] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vansonbourne.com/client-research/18091501JD.

[114] Naveen Menon, *There can be no digital economy without security*, World Economic Forum (May 8, 2017), https://www.weforum.org/agenda/2017/05/there-can-be-no-digital-economy-without-security/.

[115] *See, e.g.*, *Equifax Plummets After Huge Data Breach, Kroger Sinks on Profit drop, American Outdoor Brand Falls,* Yahoo Finance, Sept. 8, 2017, https://finance.yahoo.com/news/equifax-plummets-huge-data-breach-kroger-sinks-profit-drop-american-outdoor-brands-falls-144654294.html.

[116] *Id.*

[117] *Id.*

sess the damage and costs. However, under the FTC's current approach to Section 5 enforcement, how each business owner would be judged for liability purposes would vary greatly despite these similarities.

Under the common law of torts, absent some criminal intent (*e.g.*, insurance fraud) the businessman whose office burned down would only be held liable if he acted negligent in some way. At common law, negligence involves either an act that a *reasonable* person would know creates an unreasonable risk of harm to others.[118] Should a prosecutor or third party bring a lawsuit against the business owner, they would be required to put forth expert testimony and a detailed analysis showing exactly *how* and *why* the owner's negligence caused the fire.

Conversely, despite all of the FTC's rhetoric about "reasonableness" — which, as one might "reasonably" expect, should theoretically resemble a negligence-like framework — the FTC's approach to assessing whether a data security practice is unfair under Section 5 actually more closely resembles a rule of strict liability.[119] Indeed, rather than conduct any analysis showing that (1) the company owed a duty to consumers and (2) *how* that the company's breach of that duty was the cause of the breach — either directly or proximately— which injured the consumer, instead, as one judge noted, the FTC "kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…."[120]

There is no level of prudence that can avert *every* foreseeable harm. A crucial underpinning of calculating liability in civil suits is that some accidents are unforeseeable, some damages fall out of the chain of causation, and mitigation does not always equal complete prevention. Thus our civil jurisprudence acknowledges that no amount of care can prevent *all* accidents (fires, car crashes, *etc*.), or at least the standard of care required to achieve an accident rate near zero would be wildly disproportionate, paternalistic, and unrealistic to real-world applications (*e.g.*, setting the speed limit at 5 mph).

The chaos theory also applies to the unpredictability of data breaches. Thus, if the FTC wants to regulate data security using a "common law" approach, then it must be willing to accept that certain breaches are inevitable and liability should only arise where the company was truly negligent. This is not simply a policy argument; it is the weighing of costs and benefits that Section 5(n) requires — at least in theory. Companies do not want to be hacked any

---

[118] *See* Restatement (Second) of Torts § 284 (1965).

[119] *See* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standard-Less Data Security Standard*, Journal of Law, Economics and Policy, Forthcoming (Aug. 31, 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041533.

[120] Transcript of Proceedings at 91, 94–95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014).)).

more than homeowners want their houses to burn down. The FTC should begin its analysis of data security cases with that incentive in mind, and ask whether the company has acted as a "reasonably prudent person" would.

This, then, presents the key question: what constitutes "reasonably prudent" data security and privacy practices for purposes of avoiding liability under Section 5? To help inform Congress — and, in turn, the FTC — on how to go about answering this question, the remainder of this testimony will focus on determining three key elements of this question: (1) the types of injuries that should merit the FTC's attention, (2) the analytical framework, built upon empirical research and investigations, which should determine what constitutes "reasonable," and (3) the pleading requirements to determine the specificity with which the FTC must state its claim in the first instance.

IV. Informational Injuries In Practice: Data Security & Privacy Enforcement to Date

In 2005, the FTC brought its first data security case premised solely on unfairness — against a company (BJ's Warehouse) not for violating the promises it had made to consumers, but for the underlying adequacy of its data security practices.[121] Whether this was a proper use of Section 5 is not the important question — although it is essential to note that *BJ's Warehouse* was the consent decree that launched the FTC's use of unfairness for data security.a thousand" more (or closer to "hundreds" in the context of privacy and data security). Even if one stipulates that the FTC could have, and likely *would* have, prevailed on the merits, had the case gone to trial, the important question is this: how might the Commission have changed its approach to data security? That question becomes even more salient if one tries to project back, asking what the Commission should have done then if it had known what we know today: that twelve years later, we would still not have a single tech-related unfairness case resolved on the merits (and only four that had made it to federal court).[122]

The Commission had, of course, asked Congress for comprehensive privacy legislation in 2000.[123] Besides asking again, what else could the Commission have done? It could have be-

[121] Fed. Trade Comm'n, *BJ's Wholesale Club Settles FTC Charges* (June 16, 2005), *available at* https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

[122] *See Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017); *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 253 (3d Cir. 2015); *LabMD, Inc. v. F.T.C.*, No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd,* 776 F.3d 1275 (11th Cir. 2015); *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[123] Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Market Place- A Report to Congress* (2000) [hereinafter Privacy Report].

gun a rulemaking under the Magnusson-Moss Act of 1975, subject to the procedural safeguards imposed by Congress in 1980 (after the FTC's abuse of its rulemaking powers in the intervening five years). But, as many have noted, it would be difficult to craft prescriptive rules for data security or privacy in any rulemaking, and the process would have taken several years.

There *was* a third way: the FTC could have sought public comment on the issues of data security and privacy, issued a guidance document, then repeated the process every few years to update the agency's guidance to reflect current risks, technologies, and trade-offs. In short, the Commission could have followed the model established by its Green Guides.

V. The Green Guides as Model for Empirically Driven Guidance

As the FTC proceeds with Chairman Ohlhausen's plans for a workshop on "informational injuries," it should consider its own experience with the Green Guides as a model. The parallel is not exact: the Guides focus entirely on deception, and primarily on consumer expectations, while the FTC's proposed "informational injuries" would involve both deception and unfairness. However, the Guides do still delve into substantiation of environmental marking claims, and, thus, the underlying merits of what companies were promising their customers. FTC guidance on the meaning of "informational injuries" in the context of data security and privacy would necessarily cover wider ground, ultimately attempting to understand harms as well as "reasonable" industry practices under both deception and unfairness prongs. Still, the Guides emphasis on empirical substantiation would serve the FTC well in attempting to provide a clearer analytical basis for *why* a practice or action is deemed to have caused "informational injury" in certain cases, rather than merely stating *what* practices the FTC has determined likely to cause such harm.

Though court guidance in this context may seem rarer than the birth of a giant panda, the Third Circuit nonetheless provided some insight into the value of previous FTC guidance — namely the FTC's 2007 guidebook titled "Protecting Personal Information: A Guide for Business," — in understanding harms and "reasonable" practices that constitute violations of Section 5.[124] Discussing this guidebook, which "describes a 'checklist[]' of practices that form a 'sound data security plan,'" the court notably found that, because "[t]he guidebook does not state that any particular practice is required by [Section 5]," it, therefore, "could not, on its own, provide 'ascertainable' certainty' of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[125] Despite this recognition, the court still noted that the

[124] *Wyndham*, 799 F.3d at 256.

[125] *Id*. at 256 n.21.

guidebook did "counsel against many of the specific practices" alleged in that specific case, and thus, provided sufficient guidance in that very narrow holding to inform the defendant of "what" conduct was not considered reasonable.[126] Specifically, the court noted that the guidebook recommended:

> [T]hat companies "consider encrypting sensitive information that is stored on [a] computer network ... [, c]heck ... software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through the firewall and what they will be allowed to see ... to allow only trusted employees with a legitimate business need to access the network." It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like ... the software's default password[ ] and other easy-to-guess choices." And it recommends implementing a "breach response plan," *id.* at 16, which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information."[127]

Most notably, nowhere in the court's discussion did it identify a single instance of the FTC explaining *why* a certain practice is necessary or reasonable; instead the FTC had merely asserted that companies should just accept the FTC's suggestions, without any consideration or analysis as to whether the immense costs that might be associated with implementing many of these practices are in the consumers' best interest. This is far from the weighing of costs and benefits that Section 5(n) requires. By comparison, the Green Guides, while focused on deception, reflect a deep empiricism about substantiation of environmental marketing claims, informed by a notice and comment process and distilled into clear guidance accompanied by detailed analysis.

While multi-national corporations such as Wyndham *might* (arguably) possess the resources to blindly implement any and all suggestions the FTC makes, and to follow the FTC's pronouncements in each consent decree, the economic principle of scarcity will inevitably require smaller businesses with vastly fewer resources to make difficult decisions as to which practices they should utilize to provide the greatest security possible with its limited resources. For example, using the list above, would a company with limited resources be acting "reasonable" if it implemented a "breach response plan," but failed to check *every* software vendors' website regularly for alerts? Further, would a company be engaging in "deceptive"

[126] *Id*. at 256-57.

[127] *Id.* (internal citations omitted).

practices if it failed to notify customers that, due to limited resources, it could only implement half of the FTC's recommended practices? The answer to these questions matter and will undoubtedly have significant consequences on how competitive small businesses remain in this country. As mentioned earlier, one study suggests that 76% of customers "would move away from companies with a high record of data breaches," with 90% responding that "there are apps and websites that pose risks to the protection and security of their personal information."[128] This shows that consumers are understandably concerned about how well a company protects their data. If a company is essentially required to choose between admitting that it lacks the resources to implement advanced security practices on par with large, established businesses, or risk an FTC action for "deception," how can any startup or small business expect to compete and grow in these polarizing circumstances?

Under the FTC's current enforcement standards, this all shows how easily small businesses may find themselves in a catch-22. On the one hand, if the business wishes to pretend it has the resources to implement the same data security standards as multi-national corporations in order to attract and maintain customers weary of their data being hacked, the business will be acting "deceptively" in the eyes of the FTC, and will be open to the costly litigation, reputational damage, and massive fines that come with it. On the other hand, if the small business wishes to be open and readily admit that, due to resource constraints, its data security practices are anemic when compared to multi-national corporations, it will be open to the loss of customers and businesses invariably linked to such claims. As this illustrates, how can any startup or small business expect to compete without the FTC providing guidance as to best practices based on empirical research — including economies of scale?

Thus, to ensure the ability of businesses to compete and make sound decisions as to the allocation of their finite resources, it is imperative that the FTC not only endeavor to provide guidance as to *what* practices are sound, but also explain *why* such practices are necessary, as well as "how much" is necessary, especially in relation to a business's size and available resources.

A. The Green Guides (1992-2012)

First published in 1992, the Guides represented the Commission's attempt to better understand a novel issue before jumping in to case-by-case enforcement. By 1991, it was becoming increasingly common for companies to tout the environmental benefits of their products. In some ways, these claims were no different from traditional marketing claims: the FTC's job was to make sure consumers "got the benefit of the bargain." But in other ways, it was less

[128] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vanson-bourne.com/client-research/18091501JD.

clear exactly what that "benefit" was — such as regarding recycling content, recyclability, compostability, biodegradability, refillability, sourcing of products, etc. Rather than asserting how much of each of these consumers *should* get, the Commission sought to ground its understanding of these concepts in empirical data about what consumers actually expected. As the Commission summarized its approach in the Statement of Basis and Purpose for the 2012 update:

> The Commission issued the Guides to help marketers avoid making deceptive claims under Section 5 of the FTC Act. Under Section 5, a claim is deceptive if it likely misleads reasonable consumers. Because the Guides are based on how consumers reasonably interpret claims, consumer perception data provides the best evidence upon which to formulate guidance. As EPA observed, however, perceptions can change over time. The Guides, as administrative interpretations of Section 5, are inherently flexible and can accommodate evolving consumer perceptions. Thus, if a marketer can substantiate that consumers purchasing its product interpret a claim differently than what the Guides provide, its claims comply with the law.[129]

Of course, as the Deception Policy Statement notes, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[130] Thus, the Commission immediately added the following:

> the Green Guides are based on marketing to a general audience. However, when a marketer targets a particular segment of consumers, such as those who are particularly knowledgeable about the environment, the Commission will examine how reasonable members of that group interpret the advertisement. The Commission adds language in Section 260.1(d) of the Guides to emphasize this point. Marketers, nevertheless, should be aware that more sophisticated consumers may not view claims differently than less sophisticated consumers. In fact, the Commission's study yielded comparable results for both groups.[131]

This bears emphasis because many speak of privacy-sensitive consumers as a separate market segment, and argue that we should apply deception in privacy cases based upon their expectations. But here, unlike in privacy, the Commission actually undertook empirical research — which turned not to support an idea that probably seemed intuitively obvious: that

---

[129] Fed Trade Comm'n, Statement of Basis and Purpose (2012 Update), *at* 24-25, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguidesstatement.pdf [hereinafter "Statement of Basis and Purpose"].

[130] Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1983), *at* 1, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[131] *See* Statement of Basis and Purpose, *at* 25.

more environmentally knowledgeable or "conscious" consumers had different interpretation of environmental marketing claims.

The Commission issued the first Green Guides in August 1992, thirteen months after two days of public hearings, including a 90-day public comment period in between. The Commission followed this process in issuing revised Green Guides in 1996, 1998, and 2012. So detailed was the Commission's analysis, across so many different fact patterns, that, while the 2012 Guides ran a mere 12 pages in the Federal Register,[132] the Statement of Basis and Purpose for them ran a staggering 314 pages.[133] In each update, the FTC explored how the previous version of the Guides addresses each, the FTC's proposal, comments received on the proposal and justification for the final rule. In short, the FTC was doing something a lot like rulemaking. Except, of course, the Guides are not themselves legally binding.

The FTC has never done anything even resembling this type of comprehensive guide for data security or privacy. Indeed, just this year, the FTC touted "a series of blog posts" as a grand accomplishment in the FTC's "ongoing efforts to help businesses ensure they are taking reasonable steps to protect and secure consumer data."[134] The FTC has regularly trumpeted its 2012 Privacy Report, but that document does something very different. Most notably, the Report calls on industry actors to self-police in the most general of terms, making statements like "to the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work."[135] Unlike the focus on substance and comprehensiveness of the Green Guides, the 2012 Privacy Report speaks in generalities, dictating "areas where the FTC will be active," such as in monitoring Do Not Track implementation or promoting enforceable self-regulatory codes.[136] The lack of a Statement of Basis and Purpose akin to that issued in updating the Green Guides (the 2012 Statement totaled a whopping 314 pages) introduces unpredictability into the enforcement process, and chills industry action on data security and privacy.

---

[132] 16 C.F.R. 260 (2012).

[133] *See generally* note *129*.

[134] Press Release, Fed. Trade Comm'n, Stick with Security: FTC to Provide Additional Insights on Reasonable Data Security Practices (July 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/stick-security-ftc-provide-additional-insights-reasonable-data.

[135] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), *at* 73, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. [hereinafter "2012 Privacy Report"].

[136] *Id.* at 72.

In all, the Green Guides offer a clear, workable model for how the FTC could provide empirically grounded guidance on data security and privacy — even without any action by Congress. The key steps in issuing such guidance would be:

1. Study current industry practices across a wide range of businesses;
2. Gather data on consumer *expectations*, rather than making assumptions about consumer preferences;
3. Engage the Bureau of Economics and the FTC's growing team of in-house technologists in analysis of the costs and benefits of practice; and
4. Issue (at least) biennial or triennial guidance to reflect the changing nature, degree, and applicability of data security and privacy regulations.

Short of rulemaking, this rulemaking-like approach offers the most clarity, comprehensibility, and predictability for both FTC enforcement staff and industry actors.

B. What the Commission Said in 2012 about Modifying the Guides

There is an obvious tension between conducting thorough empirical assessments to inform updating Commission guidance and how often that guidance can be updated: the more regular the update, the more difficult it will be to for the Commission to maintain methodological rigor in justifying that update. The 2012 Statement of Basis and Purpose noted requests that the Commission review and update the Guides every two or three years, but concluded:

> Given the comprehensive scope of the review process, the Commission cannot commit to conducting a full-scale review of the Guides more frequently than every ten years. The Commission, however, need not wait ten years to review particular sections of the Guides if it has reason to believe changes are appropriate. For example, the Commission can accelerate the scheduled review to address significant changes in the marketplace, such as a substantial change in consumer perception or emerging environmental claims. When that happens, interested parties may contact the Commission or file petitions to modify the Guides pursuant to the Commission's general procedures.[137]

This strikes a sensible balance. Unfortunately, this is not at all how the Commission has handled modification of the 2012 Green Guides. Within a year, the FTC would modify the Green guides substantially with no such process for empirical substantiation to justify the new change. And this year, not five years after the issuance of the Guides, it modified the Guides yet again.

[137] *See* Statement of Basis and Purpose, *at* 26-27.

VI. Eroding the Green Guides and their Empirical Approach

While the Green Guides offer a model for empirically grounded consumer protection, the Commission has gradually moved away from that approach since issuing its last update to the Green Guides in 2012 — following an approach that more closely resembles its approach to data security and privacy.

A. Modification of the Green Guides by Policy Statement (2013)

In 2013, FTC issued an enforcement policy statement clarifying how it would apply the Green Guides,[138] updated just the year after taking notice-and-comment, to architectural coatings such as paint. The Commission appended this Policy Statement onto its settlement with PPG Architectural Finishes, Inc. ("PPG") and The Sherwin-Williams Company ("Sherwin-Williams") to settle alleged violations of Section 5 for marketing paints as being "Free" of Volatile Organic Compounds (VOCs).[139] Specifically, the Policy Statement focused on application of the 2012 Green Guides' trace-amount test, which provided:

> Depending on the context, a free-of or does-not-contain claim is appropriate even for a product, package, or service that contains or uses a trace amount of a substance if: (1) the level of the specified substance is no more than that which would be found as an acknowledged trace contaminant or background level; (2) the substance's presence does not cause material harm that consumers typically associate with that substance; and (3) the substance has not been added intentionally to the product.[140]

The Policy Statement made two clarifications specific to architectural coatings:

> First, the "material harm" prong specifically includes harm to the environment and human health. This refinement acknowledges that consumers find both the environmental and health effects of VOCs material in evaluating VOC-free claims for architectural coatings.

---

[138] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings (Mar. 6, 2013), https://www.ftc.gov/sites/default/files/ documents/cases/2013/03/130306ppgpolicystatement.pdf.

[139] Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges Against The Sherwin-Williams Co. and PPG Architectural Finishes, Inc.; Issues Enforcement Policy Statement on "Zero VOC" Paint Claims (Mar. 6, 2013), https://www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-orderssettling-charges-against-sherwin.

[140] 16 C.F.R. § 260.9(c) (2012).

> Second, the orders define "trace level" as the background level of VOCs in the ambient air, as opposed to the level at which the VOCs in the paint would be considered "an acknowledged trace contaminant." The harm consumers associate with VOCs in coatings is caused by emissions following application. Thus measuring the impact on background levels of VOCs in the ambient air aligns with consumer expectations about VOC-free claims for coatings.[141]

In both respects, the Policy Statement amended the Green Guides — while purporting merely to mirror the Guides. Most notably, the Guides had always been grounded in claims about environmental harms. For example, the Statement of Basis and Purpose for the 2012 Update had said:

> In this context [the "free of" section of the Guides"], the Commission reminds marketers that although **the Guides provide information on making truthful environmental claims**, marketers should be cognizant that consumers may seek out free-of claims for non-environmental reasons. For example, as multiple commenters stated, chemically sensitive consumers may be particularly likely to seek out products with free-of claims, and risk the most grievous injury from deceptive claims.[142]

But now the FTC's enforcement framework would, for the first time, focus on "human health" as well. In principle, this is perfectly appropriate: after all, "Unjustified consumer injury is the primary focus of the FTC Act," as the Unfairness Policy Statement reminds us.[143] But note that the Commission was *not* bringing an unfairness claim — which would have required satisfying the cost-benefit analysis of Section 5(n). Instead, the Commission was bringing a pure deception claim, as with any Green Guides claim. But unlike deception cases brought under the Green Guides, the Commission provided none of the kind of empirical evidence about how consumers understood green marketing claims that had informed the Green Guides. The Commission did not seek public comment on this proposed enforcement policy statement, nor did it supply any such evidence of its own.

In short, the 2013 Policy Statement represented not merely a *de facto* amendment of the Green Guides, undermining the precedential value of the Guides and of all other FTC guidance documents, but a break with the empirical approach by which the FTC had developed

---

[141] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings, *at* 2, https://www.ftc.gov/sites/default/files/documents/public_statements/voc-free-claims-architectural-coatings/130306ppgpolicystatement.pdf.

[142] *See* Statement of Basis and Purpose, *at* 138 n. 469.

[143] 1980 Unfairness Policy Statement.

the Guides since 1992. This alone should call into question the FTC's willingness, in recent years, to ground consumer protection work in empirical analysis. But worse was yet to come.

B. Modification of the Green Guides by Re-Opening Consent Decree (2017)

This July, Ohlhausen, now Acting Chairwoman, effectively proposed amending the FTC's Green Guides — first issued in 1992 and updated in 1996, 1998 and 2012 — via proposed consent orders issued to four paint companies accused of deceptively promoting emission-free or zero volatile organic compounds in violation of Section 5 of the FTC Act.[144] In the corresponding press release, the Commission said it plans to "propose harmonizing changes to two earlier consent orders issued in the similar PPG Architectural Finishes, Inc. (Docket No. C-4385) and the Sherwin Williams Company (Docket No. C-4386) matters," and plans to "issue orders to show cause why those matters should not be modified pursuant to Section 3.72(b) of the Commission Rules of Practice, 16 C.F.R. 3.72(b)," if the consent orders are finalized.[145]

This repeated, and compounded, the two sins committed by the FTC in 2013: (1) undermining the value of Commission guidance (here, both the 2012 Guides and the 2013 Enforcement Policy Statement) by reminding all affected parties that guidance provided one day can be changed or revoked the next and (2) failing to provide empirical substantiation for its new approach. To these sins, the Commission added two more: (3) revoking guidance that had been treated as authoritative, and relied upon, by regulated parties for the previous four years through a consent decree and (4) re-opening the two consent decrees to which the 2013 Enforcement policy was attached to "harmonize" them with the FTC's new approach. Revoking guidance treated as authoritative raises fundamental constitutional concerns about "fair notice." Re-opening consent decrees raises even more serious concerns about the FTC's process.

These concerns are reflected in recently proposed FTC settlements. In the 2013 PPG and Sherwin-Williams consent orders, the Commission specified the scope of its jurisdiction in Article II of the orders, stating:

---

[144] Press Release, Fed. Trade Comm'n, Paint Companies Settle FTC Charges That They Misled Consumers; Claimed Products Are Emission- and VOC-free and Safe for Babies and other Sensitive Populations, (July 11, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/07/paint-companies-settle-ftc-charges-they-misled-consumers-claimed.

[145] *Id.* at ¶ 13.

> IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any covered product in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, regarding:
>
> A. The VOC level of such product; or
>
> B. Any other *environmental* benefit or attribute of such product,
>
> unless the representation is true, not misleading, and, at the time it is made, respondent possesses and relies upon competent and reliable scientific evidence that substantiates the representation.[146]

In the same orders, the Commission defined "trace" levels of VOCs as including a "human health" component, stating:

> 7. "Trace" level of VOCs shall mean:
>
> A. VOCs have not been intentionally added to the product;
>
> B. The presence of VOCs at that level does not cause material harm that consumers typically associate with VOCs, including but not limited to, harm to the environment or *human health*; and
>
> C. The presence of VOCs at that level does not result in concentrations higher than would be found at background levels in the ambient air.[147]

While the inclusion of language that specified health as a VOC-related hazard created no immediate substantive changes, it laid the groundwork for a broadening of what constitutes a legitimate claim under the definition of VOC. Specifically, this would mean that the FTC would only have to take one additional step to claim a VOC-related violation if a company did not meet some broad, amorphous standard of "human health" conceived by the FTC. In fact, the 2017 Benjamin & Moore Co., Inc., ICP Construction Inc., YOLO Colorhouse LLC, and Imperial Paints, LLC consent orders took this additional step in an updated Article II, stating:

> IT IS FURTHER ORDERED that Respondent …. must not make any representation, expressly or by implication … regarding:

---

[146] Fed. Trade Comm'n, *In the Matter of PPG Architectural Finishes, Inc.*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025ppgagree.pdf; *see also* Fed. Trade Comm'n, *In the Matter of Sherwin-Williams Company*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025sherwinwilliamsagree.pdf.

[147] *Id.* at 3.

A. The emission of the covered product;

B. The VOC level of the covered product;

C. The odor of the covered product;

D. *Any other health benefit or attribute* of, or risk associated with exposure to, the covered product, including those related to VOC, emission, or chemical composition; or

E. Any other environmental benefit or attribute of the covered product, including those related to VOC, emission, or chemical composition, unless the representation is non-misleading, including that, at the time such representation is made, Respondent possesses and relies upon competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence, to substantiate that the representation is true.

Given the nature and type of these products, it is possible that health-related hazards should have been included in these particular consent orders. This would imply that it is the specific context of these cases that serves as a justification for the inclusion of the health-related language. However, the harmonization of these new orders with the 2013 PPG and Sherwin-Williams orders would create new, broader obligations on those two companies. More generally, this would imply that the basis of the FTC's authority emanates not from the context in which the claim is brought, but instead from the very nature of VOCs, i.e. as newly-deemed health hazards.

As a general principle, this means that, under its deception authority, the FTC could create *ex post facto* justifications for expanding its enforcement powers arbitrarily and with no forward guidance. For example, although the voluminous 2012 Green Guides Statement of Basis and Purpose made no mention of health risks,[148] the Commission found a way to add it on to previous consent agreements in a unilateral, non-deliberative way. This places industry actors at the mercy of the FTC, which can alter previous consent orders based on present or future interpretations of "deception."

C. Remember Concerns over Revocation of the Disgorgement Policy?

It is ironic that it should be this particular FTC that would modify a Policy Statement, which was treated as authoritative by regulated parties for four years and which was itself a surreptitious modification of a Guide issued through public notice and comment (and resulting

[148] *See generally* Statement of Basis and Purpose.

in a 314-page Statement of Basis and Purpose), through such summary means — given that Acting Chairman Ohlhausen had previously urged greater deliberation and public input in withdrawing a policy statement.

In July 2012, the FTC summarily revoked its 2003 Policy Statement on Monetary Equitable Remedies in Competition Cases (commonly called the "Disgorgement Policy Statement")[149] on a 2-1 vote.[150] Commissioner Ohlhausen, the sole Republican on the Commission at the time, objected: "we are moving from clear guidance on disgorgement to virtually no guidance on this important policy issue."[151] She also objected to the cursory, non-deliberative nature of the underlying process:

> I am troubled by the seeming lack of deliberation that has accompanied the withdrawal of the Policy Statement. Notably, the Commission sought public comment on a draft of the Policy Statement before it was adopted. That public comment process was not pursued in connection with the withdrawal of the statement. I believe there should have been more internal deliberation and likely public input before the Commission withdrew a policy statement that appears to have served this agency well over the past nine years.[152]

What then-Commissioner Ohlhausen said then about revocation of a policy statement remains true now about substantial modification of a policy statement (which is effectively a partial withdrawal of previous guidance): both internal debate and public input are essential. Burying the request for public comment in a press release about new settlements hardly counts as an adequate basis for reconsidering the 2013 Policy Statement — let alone modifying the 2012 Green Guides.

D. What Re-Opening FTC Settlements Could Mean for Tech Companies

The Commission could have, at any time over the last twenty years, undertaken the kind of empirical analysis that led to the Green Guides, and published guidance about interpretation of Section 5, but never did so. Instead, the Commission issued only a series of reports making broad, general recommendations. In fact, in one of the only two data security cases not to

---

[149] Fed. Trade Comm'n, Policy Statement on Monetary Equitable Remedies in Competition Cases, 68 Fed. Reg. 45,820 (Aug. 4, 2003).

[150] Press Release, Fed. Trade Comm'n, FTC Issues Policy Statement on Use of Monetary Remedies in Competition Cases (July 31, 2003), available at http://www.ftc.gov/opa/2003/07/disgorgement.shtm.

[151] *See* Statement of Commissioner Maureen K. Ohlhausen Dissenting from the Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases, *at* 2 (July 31, 2012), https://www.ftc.gov/public-statements/2012/07/statement-commissioner-maureen-k-ohlhausen-dissenting-commissions-decision.

[152] *Id.* at 2.

end in a consent decree, a federal district judge blasted the FTC's decision not provide *any* data security standards:

> No wonder you can't get this resolved, because if [a 20-year consent order is] the opening salvo, even I would be outraged, or at least I wouldn't be very receptive to it if that's the opening bid…. You have been completely unreasonable about this. And even today you are not willing to accept any responsibility…. *I think that you will admit that there are no security standards from the FTC*. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…. [H]ow does any company in the United States operate when . . . [it] says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did…. *[Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required*. You are a regulatory agency. I suspect you can do that.[153]

In recent years, the Commission has proudly trumpeted its "common law of consent decrees" as providing guidance to regulated entities.[154] Now, everyone must understand that those consent decrees may be modified at any time, particularly those consent decrees that are ordered by the Commission (as opposed to a federal court). As the Supreme Court made clear, "[t]he Commission has statutory power to reopen and modify its orders at all times."[155] In order to reopen and modify an order, the Commission faces an incredibly low bar, having to merely show that it has "reasonable grounds to believe that public interest at the present time would be served by reopening."[156] Meanwhile, the FTC's consent decrees often stipulate that the defendant "waives… all rights to seek judicial review or otherwise challenge or contest the validity of the order entered pursuant to this agreement."[157]

---

[153] Transcript of Proceedings at 91, 94-95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014)) (emphasis added).

[154] Julie Brill, Comm'r, Fed. Trade Comm'n, "Privacy, Consumer Protection, and Competition," Address at the 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-and-competition/120427loyolasymposium.pdf (stating the FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow").

[155] Atl. Ref. Co. v. F.T.C., 381 U.S. 357, 377 (1965).

[156] *Elmo Co. v. F.T.C.*, 389 F.2d 550, 552 (D.C. Cir. 1967), *cert. denied*, 392 U.S. 905 (1968).

[157] *See, e.g.,* Agreement Containing Consent Order at 3(C), In re Oracle, No. 132 3115 (F.T.C. Dec. 21, 2015), https://www.ftc.gov/system/files/documents/cases/151221oracleorder.pdf.

But in cases where the FTC needs a court to issue a consent decree (e.g., to obtain an injunction or restitution), if the FTC wishes to modify the decree, it must at least meet the requirements imposed by Federal Rule of Civil Procedure 60:[158] the FTC must meet a heightened pleading standard through a showing of, for example, "fraud," "mistake," or "newly discovered evidence" necessitating such a modification.[159] Furthermore, the FTC does not have the freedom to modify court ordered consent decrees "at any time," as with settlements, but must file a motion "within a reasonable time" — the same standard that applies to all litigants in federal court.[160]

Why should there be such radically different standards? It is true that violating court-ordered consent decrees can result in criminal liability penalties, while violating Commission-ordered consent decrees means only civil penalties — but those penalties may be significant. For example, in 2015, the FTC imposed a $100 million fine against Lifelock for violating a 2010 consent decree by failing to provide "reasonable" data security[161] — over eight times the amount of the company's 2010 settlement and two thirds of the company's entire revenue that quarter ($156.2 million).[162] In general, arbitrarily-imposed, post-hoc civil liability carries the risk of causing significant economic loss, reputational harm, and even business closure. For example, the Commission could re-open *all* its past data security and privacy cases to modify the meaning of the term "covered information." To the extent that companies are found to be in non-compliance with the new standard, they would be liable for prosecution to the full extent of the FTC's powers. Besides compromising the ability of existing industry actors to comply, invest, and grow, this would have the effect of deterring new actors from entering a data-based industry for fear of uncertainty and retroactive prosecution.

Congress should reassess the standard by which the FTC may reopen and modify its own orders. In doing so, it should begin with the question articulated long ago by the Supreme Court: "whether any thing has happened that will justify … changing a decree."[163] In answering this question, the Court made clear that "[n]othing less than a clear showing of grievous

---

[158] Fed. R. Civ. P. 60 (stating that "the court may relieve a party or its legal representative from a final judgment, order, or proceeding" for certain reasons, including "mistake," "newly discovered evidence," "fraud," and "any other reason that justifies relief.").

[159] Fed. R. Civ. P. 60(b).

[160] Fed. R. Civ. P. 60(c).

[161] Fed. Trade Comm'n, *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order* (Dec. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

[162] LifeLock, Inc., *LifeLock Announces 2015 Fourth Quarter Results* (Feb. 10, 2016), *available at* https://www.lifelock.com/pr/2016/02/10/lifelock-announces-2015-fourth-quarter-results-2/

[163] *United States v. Swift & Co*., 286 U.S. 106, 119 (1932).

wrong evoked by new and unforeseen conditions should lead us to change what was decreed ... with the consent of all concerned."[164] The reason for the Court's hesitation to modify consent decrees should be obvious: despite retaining the force of a court order, consent decrees are, at their core, stipulated terms *mutually* agreed to by the parties to the litigation, similar to traditional settlements of civil litigation. Thus, by choosing to settle and enter into consent decrees, "[t]he parties waive their right to litigate the issues involved in the case and thus save themselves the time, expense, and inevitable risk of litigation."[165]

In federal court, Rule 60 forces parties to show that circumstances have indeed changed enough to justify modification of a court order. However, having to only show that it believes the "public interest" would be served, the FTC essentially is not required to make *any* showing of necessity that would counterbalance the value of preserving the terms of the settlement. Given the enormous weight the FTC itself has placed upon its "common law of consent decrees," as a substitute both for judicial decisions and clearer guidance from the agency, Congress should find it alarming that the FTC is now undermining the value of that pseudo-common law.

Ultimately, allowing the FTC to modify such agreements without showing any real cause not only negates the value of such agreements to each company (in efficiently resolving the enforcement action and allowing the company to move on), but more systemically and perhaps more importantly, it diminishes the public's trust in the government to be true to its word. Procedure matters. When agencies fail to utilize fair procedures in developing laws, the public's faith in both the laws and underlying institutions is diminished. This, in turn, undermines their effectiveness and further erodes the public's trust in the legal institutions upon which our democracy rests.[166] Thus, even in instances where the policy behind the rule may be sound, a failure by the implementing agency to follow basic due process will undermine the public's faith and deprive businesses of the certainty they need to thrive.[167]

---

[164] *Id*.

[165] *Local No. 93, Int'l Asso. of Firefighters, etc. v. Cleveland*, 478 U.S. 501, 522 (1986) (quoting *United States v. Armour & Co.*, 402 U.S. 673, 681-682 (1971)).

[166] *See, e.g*, Pew Research Center, Beyond Distrust: How Americans View Their Government (2015) ("Only 19% of Americans today say they can trust the government in Washington to do what is right "just about always" (3%) or "most of the time" (16%).").

[167] *See, e.g., Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974) (recognizing that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible).

VII. Better Empirical Research & Investigations

Why *doesn't* the FTC do more empirical research — the kind that went into the Green Guides? What should the process around, and following, its forthcoming workshop on "informational injuries" look like?

A. What the FTC Does Now

Since 2013, the FTC has published each January an annual report titled the "Privacy & Data Security Update."[168] The 2016 Report[169] boasts the FTC's "unparalleled experience in consumer privacy enforcement[170]" and the wide spectrum of offline, online, and mobile privacy practices that the Commission has addressed with enforcement actions:

> [The FTC] has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.[171]

Given the far-reaching scope of the FTC's jurisdiction on Section 5 enforcement and the wide range of companies that have settled "informational injury" cases, one might expect the these annual "Updates" to do more than merely summarize the previous year's activities, and instead provide empirical research into the privacy and data threats facing consumers. By failing to do so, the Commission not only leaves businesses in the dark as to what constitutes "reasonable" practices in the Government's eyes, but fails to inform them of the best practices available to ensure that Americans' data and privacy is adequately protected.

For example, if the Commission is to proudly report that consumer protection was achieved from settling charges with a mobile ad network on the grounds that "[the company] deceived consumers by falsely leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones,"[172] that Commission's work should not have ended there as a single bullet-point of the Commission's many highlights. As an

---

[168] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2013 (June 2012), *available at* https://www.ftc.gov/policy/reports/policy-reports/commission-and-staff-reports?title=data+security&items_per_page=20.

[169] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2016 (Jan 2017), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2016.

[170] *Id*. *at* 2.

[171] *Id*.

[172] *Id.*

enforcement agency with vast interpretive powers on deceptive practices, and an investigative body with considerable analytical resources, the Commission has a further duty to clearly explain the empirical rationale that substantiates the settlement: Just how do consumers understand privacy in the use of advertising cookies? How might companies use Do Not Track signals, given those consumer expectations, to provide an effective opt-out mechanism? How should the standard differ based on the sizes of companies and the services they provide? What "informational injuries" occur when consumers unknowingly receiving tailored advertisements through the use of unique device identifiers? It is one thing to say that the Commission should not have to answer all these questions in its pleadings, or even in order to prevail in a deception case. It is quite another to say that the Commission should not be expected to perform any research even after the fact, especially on matters that recur across a larger arc of enforcement actions.

Unforeseen vulnerabilities are the inevitable side-effect of rapid technological advancements; in the area of data privacy and security, new consumer risks will arise continually, raising questions that *should* merit careful quantitative and qualitative analyses. However, in its "Privacy & Data Security Update," the FTC essentially asserts an answer without "showing its work."

This is in stark comparison to the FTC's approach on the Green Guides, where "the Commission sought comment on a number of general issues, including the continuing need for, and economic impact of, the Guides, as well as the Guides' effect on environmental claims":[173]

> [B]ecause the Guides are based on consumer understanding of environmental claims, consumer perception research provides the best evidence upon which to formulate guidance. The Commission therefore conducted its own study in July and August of 2009. The study presented 3,777 participants with questions calculated to determine how they understood certain environmental claims. The first portion of the study examined general environmental benefit claims ("green" and "eco-friendly"), as well as "sustainable," "made with renewable materials," "made with renewable energy," and "made with recycled materials" claims. To examine whether consumers' understanding of these claims differed depending on the product being advertised, the study tested the claims as they appeared on three different products: wrapping paper, a laundry basket, and kitchen flooring. The second portion of the study tested carbon offset and carbon neutral claims.[174]

Here is an excellent example of the FTC's use of consumer perception data to study the effect of environmental labels, with variables on consumer behavioral segments and changes on

[173] Statement of Basis and Purpose, *at* 8.

[174] *Id.* at 9-10.

perception over time, to substantiate deception claims. Even with the empirical research grounded in a large sample size, the Commission continued to reanalyze "claims appearing in marketing on a case-by-case basis because [the Commission] lacked information about how consumers interpret these claims."[175] The "Green Guides: Statement of Basis and Purpose"[176] is a 314 page document that comprehensively reviews the Commission's economic and consumer perception studies and weighs different empirical methodologies on the appropriate model of risk assessment. It meaningfully fleshes out the Green Guides' core guidance on the "(1) general principles that apply to all environmental marketing claims; (2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and (3) how marketers can qualify their claims to avoid deceiving consumers," with self-awareness of the economic impact of regulations and a robust metric on consumer expectations to materialize the Commission's enforcement policies.

It is deeply troubling that this level of thoroughness evades the Commission's privacy enforcement, where the toolbox of economics remains unopened in managing the information flows of commercial data in boundless technology sectors pervading everyday life. The FTC's history of consent decrees provides nothing more than anecdotal evidence that *some* guiding principle is present, within the vague conceptual frameworks of "privacy by design," "data minimization", or "notice and choice."[177]" Data privacy and security regulations do not exist in a silo, abstracted and harbored from real-life economic consequences for the consumers, firms, and stakeholders—whose interests intersect at the axis of the costs and benefits of implementing privacy systems, the need for working data in nascent industries, and the market's right to make informed decisions. Consumer protection through privacy regulation is undoubtedly a matter of economic significance parallel to antitrust policies or the label marketing in the Green Guides. Personally identifiable information ("PII") is a valuable corporate asset like any other,[178] with competitive market forces affecting how it is processed, shared, and retained. Modern consumers are cognizant of the tradeoffs they make at the convenience of integrated technology services, and the downstream uses of their data. Accordingly, not every technical deviation from a company's privacy policy is an affront to consumer welfare that causes "unavoidable harms not outweighed by the benefits to consumers or competition."[179] The FTC has too long failed to articulate the privacy risks it intends to rectify, nor to

[175] *See* Statement of Basis and Purpose, *at* 27.

[176] *See generally* Statement of Basis and Purpose.

[177] *See generally* 2012 Privacy Report.

[178] Clearwater Compliance LLC, *The Clearwater Definition of an Information Asset*, https://clearwatercompliance.com/wp-content/uploads/2015/11/Clearwater-Definition-of-Information-Assets-with-Examples_V8.pdf.

[179] 12 U.S.C. § 5331(c)(1).

quantify the "material" consumer harm through behavioral economics or any empirical metric substantiated beyond its usual *ipso facto* assertion of deception.

B. The Paperwork Reduction Act

A noteworthy legislation that defined the FTC's administrative authority after Congress imposed additional safeguards upon the FTC's Magnuson-Moss rulemaking powers in 1980 is the Paperwork Reduction Act of 1980 ("PRA").[180] These two 1980 enactments must be understood together as embodying Carter-era attempts to reduce the burdens of government. Specifically, Congress intended the PRA to serve as an administrative check on the Federal agency's information collection policy, with the goal of reducing paperwork burdens for individuals, businesses, and nonprofits by requiring the FTC to seek clearance from the Office of Management and Budget ("OMB") on compulsory process orders surveying ten or more members of the public.

The "collection of information" that falls under the constraints of the PRA is defined as:

> the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either— answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States.[181]

Some have claimed that the PRA has hampered the FTC's ability to collect data from companies and thus to perform better analysis of industry practices, informational injuries, and the like. The FTC's power to gather information *without* "a specific law enforcement purpose" derives from Section 6(b) of the FTC Act, which the FTC has summarized in relevant part as follows:

> Section 6(b) empowers the Commission to require the filing of "annual or special reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of the entities to whom the inquiry is addressed. [182]

---

[180] Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501–3520 (2012)).

[181] 44 U.S.C. § 3502(3).

[182] Fed. Trade Comm'n, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (July 2008), *available at* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

Such reports would certainly be helpful for providing better substantiated guidance regarding data privacy and security practices. It is worth carefully considering what the PRA requires and how it might affect the FTC's collection of data. There is indeed some circumstantial evidence to suggest that the FTC may be structuring its 6(b) inquiries to avoid the PRA, by limiting the number of firms from which the FTC requests data to fewer than ten[183] — the threshold for triggering the PRA's requirements.

A case study on the FTC's survey of Patent Assertion Entities ("PAEs")[184] illustrates two potential ways the PRA might affect the FTC's collection of empirical data and thus the quality of its analysis and guidance in data security and privacy cases. First, by its own terms, the PRA applies even to *voluntary* data-collection of the sort that could allow the FTC compile "line of business" studies that consider wider practices beyond a single case:

> [T]he obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency … *whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit.*[185]

The burden-minimization goal of the PRA is evaluated by the OMB based on broad, unpredictable criteria, such as whether the "the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility."[186] The PRA has been enforced by the OMB with tunnel vision on reducing the burden of paperwork and compliance, measured quite simply on the metric of man hours spent processing the paperwork.[187] However, the more important question lies on balancing the potential burden of information collection with the value of added research and empirical data on FTC policymaking. The balance was correctly struck on the Green

---

[183] *See e.g.*, FTC To Study Credit Card Industry Data Security Auditing Commission Issues Orders to Nine Companies That Conduct Payment Card Industry Screening (March 2016) https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing;
FTC To Study Mobile Device Industry's Security Update Practices (May 2016) https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[184] Layne-Farrar, Anne, What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016). Available at SSRN: https://ssrn.com/abstract=2722057. or http://dx.doi.org/10.2139/ssrn.2722057.

[185] 5 C.F.R. § 1320.3(c).

[186] United States Office of Personnel Management, Paperwork Reduction Act (PRA) Guide Version 2.0 (April 2011), available at https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

[187] *Id. See also* Sam Batkins, Evaluating the Paperwork Reduction Act: Are Burdens Being Reduced? AAF, https://www.americanactionforum.org/testimony/evaluating-paperwork-reduction-act-burdens-reduced/.

Guides, where the PRA analysis was satisfied upon a consideration of the benefits of consumer surveys which outweighed the minimal burdens to the respondents:

> Overall burden for the pretest and questionnaire would thus be 2,511 hours. The cost per respondent should be negligible. Participation is voluntary and will not require start-up, capital, or labor expenditures by respondents.[188]

Moreover, the FTC integrated various suggestions on the study methodology and data collection methods submitted in a public comment by the General Electric Company ("GE"), to ensure that the Commission surveyed "a proper universe of consumers" upon which to "obtain accurate projections of national sentiment."[189]

> With respect to GE's concern about identifying the ''proper universe of consumers,'' FTC staff has included in the questionnaire a brief section of questions that address participants' level of interest in environmental issues. For example, one question asks: ''In the past six months, have you chosen to purchase one product rather than another because the product is better for the environment?'' Through analyses of answers to such questions, staff can compare the study responses of participants who have a high degree of interest in environmental issues and who take these issues into account when making purchasing decisions with responses of participants who are not as concerned with environmental issues.
>
> GE also asserts that the FTC should ensure a ''proper sample size.'' The FTC staff determined the sample size of 3,700 consumers based on several considerations, including the funds available for the study, the cost of different sample size configurations, the number of environmental claims to be examined, and a power analysis. In this study, 150 participants will see each of the various environmental marketing claims to be compared. Staff believes that this will be adequate to allow comparisons across treatment cells.[190]

By contrast, the FTC study on PAEs, which also received PRA clearance, compiled "nonpublic data on licensing agreements, patent acquisition practices, and related costs and revenues"[191] to illuminate how PAEs operate in patent enforcement activity outside the confines

---

[188] Fed. Trade Comm'n, Agency Information Collection Activities; Submission for OMB Review; Comment Request (May 2009), Federal Register / VOL. 74, NO. 90, *available at* https://www.ftc.gov/sites/default/files/documents/federal_register_notices/green-marketing-consumer-perception-study-agency-information-collection-activities-submission-omb/090512greenmarketing.pdf.

[189] *Id* at 22398.

[190] *Id*.

[191] *See* What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016); "Supporting Statement for a Paperwork Reduction Act: Part B" *available at* http://www.reginfo.gov/public/do/DownloadDocument?objectID=47563401.

of litigation records. But even when the OMB cleared the PAE study, the FTC chose a limited sample size of "25 PAEs, 9 wireless chipset manufacturers that hold patents, and 6 non-practicing wireless chipset patent holders."[192] This restrictive sample size significantly limited the applicability of the Commission's conclusions. More broadly, it suggests a shift towards a general reluctance to design and implement systemic research even when the required administrative blessing is obtained under the PRA.

The PRA Guide of 2011 outlines information collection policies and procedures, albeit with only a superficial explanation of statistical methodologies, and zero mention of survey design and quantitative research methods. [193] It is a cause for concern that the OMB's task of cutting down on the amount of paperwork is framed so parochially, for the short term goal of reducing participation hours, without perhaps considering cases where the quality and usability of the research itself depends on obtaining a larger sample. The mandate to limit the sample size of survey respondents ironically defeats the "practical utility" of the research, which is one of the main cornerstones of the PRA.

On the other hand, the PRA does not apply to *all* voluntary collection — only when the FTC sends "identical" questions to ten or more companies (whether their answer is voluntary or compulsory). The PRA would *not* apply to the FTC requesting public comment, such as it has done through the Green Guides process. This point is critical: while targeting specific companies with the same questions might well prove useful in informing the FTC's understanding of informational injuries, the FTC's failure to collect more such data thus far, to analyze it, and to publish it in useful guidance can in no way be blamed on the requirements of the PRA. Nor can it excuse the FTC staff for relying on an expert witness in the LabMD case whose recommendations about "reasonable" data security referred exclusively to the practices of Fortune 500 companies, without referencing *any* small businesses comparable in size and technical sophistication to LabMD.[194]

Indeed, the PRA Guide exempts from the definition of "information," and thus eliminates the need for clearance on, the collection of "facts or opinions submitted in response to general solicitations of comments from the general public"[195] and "examinations designed to test the

---

[192] *Id.*

[193] *See generally* Paperwork Reduction Act (PRA) Guide Version 2.0.

[194] Gus Hurwitz, *The FTC's Data Security Error: Treating Small Businesses Like the Fortune 1000* (Feb. 20, 2017), *available at* https://www.forbes.com/sites/washingtonbytes/2017/02/20/the-ftcs-data-security-error-treating-small-businesses-like-the-fortune-1000/#58d2b735a825.

[195] United States Office of Personnel Management, Paperwork Reduction Act (PRA), Version 2.0, OPM at 6 (April 2011), *available at* https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

aptitude, abilities, or knowledge of the person tested for a collection."[196] The PRA poses no impediment to the FTC taking a proactive approach on conducting empirical research on data privacy by calling for consumer survey participants, holding public workshops, or from analyzing public data such as companies' privacy policies as a means to test privacy risk perception and consumer expectations. The Green Guides illustrate just how much data collection the FTC can do to substantiate its policymaking with empirical and economic research, based on real consumer studies.

VIII. Pleading, Settlement and Merits Standards under Section 5

In general, the FTC Act currently sets a very low bar for bringing complaints: "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[197] In practice, this has become the standard for *settlements*, since the Act does not provide such a standard, and the FTC commonly issues both together. This raises three questions:

1. What should the standard be for issuing complaints?
2. Closely related, what should the standard be for courts weighing a defendant's motions to dismiss?
3. What should the standard be for settling cases?

Raising all three bars would do much to improve the quality of the agency's "common law" in several respects:

1. It would provide greater rigor for FTC staff throughout the course of the investigation;
2. Companies would be less likely to settle, and more likely to litigate, if they had a better chance of prevailing at the motion to dismiss stage; and
3. Complaints that settle before trial (after the FTC has survived a motion to dismiss) would, or complaints that the FTC has withdrawn (after the FTC has lost a motion to dismiss) would provide more guidance standing on their own as the final, principle record of each case.

We take the questions raised above in reverse order, beginning with the standard by which a court will assess a motion to dismiss and concluding with the standard by which Commissioners will decide whether to issue a complaint (and thus, in nearly every case, also a settlement):

[196] *Id*.

[197] 15 U.S.C. 45(b).

A. Pleading & Complaint Standards

Fortunately, the courts are already moving towards requiring the FTC to do a better job of writing its pleadings (complaints) or face dismissal of its complaints — at least with respect to deception. Congress should take note of the current case law on this issue and consider codifying a heightened pleading requirement for any use of Section 5.

Heightened pleading standards can be fatal to normal plaintiffs, who need to survive a motion to dismiss in order to obtain the discovery they need to actually prevail on the merits. But the FTC has uniquely broad investigative powers. It is difficult to see why they would *ever* need court-ordered discovery — in other words, why would it be a problem for the Commission to have to do more to ground their complaints in the requirements of Section 5, as made clear in the FTC's Deception and Unfairness policy statements, and Section 5(n). Today, the FTC wants the best of both worlds: vast pre-trial discovery power *and* the low bar for pleadings claimed by normal plaintiffs who lack that power.

At a minimum, the FTC should be required to plead its Section 5 claims with specificity. Ideally, this standard would closely mirror a "preponderance of the evidence," as explained in the attached white paper.[198]

1. Deception Cases

TechFreedom has long argued that the FTC's deception complaints should have to satisfy the heightened pleading standards of Fed. R. Civ. Pro. 9(b).[199] Under that rule, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."[200] In other words, such claims must be accompanied by the "who, what, when, where, and how" of the conduct charged.[201] Rule 9(b) gives defendants "notice of the claims against them, provide[ ] an increased measure of protection for their reputations, and reduce[ ] the number of frivolous suits brought solely to extract settlements."[202]

Several district courts have concluded that 9(b) applies to FTC deception allegations.[203] Most recently, the Northern District of California dismissed two of the FTC's five deception counts

---

[198] *See* White Paper, *supra* note 51, at 18-21 (unfairness) and 28 (deception).

[199] *See* Brief of Amicus Curiae TechFreedom, International Center for Law and Economics, & Consumer Protection Scholars in Support of Defendants, *FTC. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887), 2013 WL 3739729, *available at* https://goo.gl/JGUE9e.

[200] Fed. R. Civ. P. 9(b).

[201] *Vess v. Ciba–Geigy Corp., USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

[202] In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1418 (3d Cir. 1997).

[203] *See, e.g.,* FTC v. Lights of Am., Inc., 760 F. Supp. 2d 848 (C.D. Cal. 2010); FTC v. Ivy Capital, Inc., 2011 WL 2118626 (D. Nev. May 25, 2011); FTC v. ELH Consulting, LLC, No. CV 12-02246-PHX-FJM, 2013 WL 4759267,

in its data security complaint against D-Link[204] for failure to satisfy the heightened pleading standard of Rule 9(b).[205] The district court noted that the Ninth Circuit has yet to address the question, but nonetheless found controlling the appeals court's decision holding that California's Unfair Competition Law — the state's "Baby FTC Act," which, "like Section 5 outlaws deceptive practices without requiring fraud as an essential element" — is subject to Rule 9(b).[206]

The *D-Link* court's analysis of each of the FTC's five deception counts illustrates that, while a heightened pleading standard *would* require more work from Commission staff to establish their cases, this burden would be relatively small and would in no way hamstring the Commission from bringing legitimate cases. The court upheld the principal deception count (Count II: "that DLS has misrepresented the data security and protections its devices provide") and two others, dismissing only two peripheral claims. If anything, merely applying Section 9(b) to the Commission's complaints would likely not be enough, on its own, to provide adequate discipline to the Commission's use of its investigation and enforcement powers — but it would certainly be a start.

The district court's discussion of Count II illustrates what specificity in pleading deception claims would look like. The FTC's allegations identified "specific statements DLS made at specific times between December 2013 and September 2015," and that the allegations "also specify why the statements are deceptive."[207] The court goes on to say that "Count II identifies the time period during which DLS made the statements and provides specific reasons why the statements were false—for example, that the routers and IP cameras could be hacked through hard-coded user credentials or command injection flaws," and that "this is all Rule 9(b) demands."[208]

---

at *1 (D. Ariz. Sept. 4, 2013) (same); *see also* FTC v. Swish Marketing, No. C-09- 03814-RS, 2010 WL 653486, at *2-4 (N.D. Cal. Feb. 22, 2010) (finding "a real prospect" that Rule 9(b) applies but not deciding the issue).

[204] *See* Complaint for Permanent Injunction and Other Equitable Relief, *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), https://www.ftc.gov/system/files/documents/cases/d-link_complaint_for_permanent_injunction_and_other_equitable_relief_unredacted_version_seal_lifted_-_3-20-17.pdf.

[205] *See* Order Re Motion to Dismiss, *Fed. Trade Comm'n v. D-Link Sys.,* No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), *at* 2-3, https://consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf.

[206] *Id.* at 2-3 (discussing Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1103-04 (9th Cir. 2003)).

[207] *Id.* at 4.

[208] *Id.* at 4-5.

2. Unfairness Cases

The *D-Link* court noted that "[w]hether the FTC must also plead its unfairness claim under Rule 9(b) is more debatable," finding "little flavor of fraud in the[] elements [of unfairness under Section 5(n)]." But, the court continued:

> the FTC has expressly stated that the unfairness claim against DLS is not tied to an alleged misrepresentation. See Section III, below. At the same time, however, the FTC has said that for all of its claims "the core facts overlap, absolutely," and there is no doubt that the overall theme of the complaint is that DLS misled consumers about the data security its products provide. The FTC also acknowledges that DLS's misrepresentations are relevant to the unfairness claim because consumers could not have reasonably avoided injury in light of them.
>
> Consequently, there is a distinct possibility that Rule 9(b) might apply to the unfairness claim. But the question presently is not ripe for resolution. As discussed below, the unfairness claim is dismissed under Rule 8. Whether it will need to satisfy Rule 9(b) will depend on how the unfairness claim is stated, if the FTC chooses to amend.[209]

Whatever the courts actually conclude about the applicability of Rule 9(b) to unfairness claims, we see no reason why the Commission should not be subject to the same heightened pleading requirements under unfairness.

B. Preponderance of the Evidence Standard

Applying Section 9(b) to all Section 5 pleadings would help greatly. But the more fundamental problem in unfairness cases is the low bar set by Section 5(b) for bringing a complaint — and the lack of *any* standard for settling it. We believe the answer is to require the Commission staff to demonstrate that it would prevail by a preponderance of the evidence. It may, at first, seem strange to apply this standard — the general standard for resolving civil litigation — at the early stages of litigation, but it must be remembered that this is not normal litigation. As noted above, the FTC has unique pre-trial discovery powers, and so is very likely to have accumulated all the evidence it will need at trial before the complaint is ever issued. Second, in nearly every "informational injury" case, the Commission's decision over whether to issue a complaint *is* the final decision over the case — because the cause will simply settle at that point. Congress should consider applying this standard either to the issuance of unfairness complaints, or to the issuance of settlements. If the standard is applied only to the issuance of settlements, Congress should consider some other heightened standard for

[209] *Fed. Trade Comm'n v. D-Link Sys.,* at *2 (N.D. Cal. Sept. 19, 2017).

bringing unfairness complaints, above that required by Section 9(b). In any event, the purpose of any standard imposed at this stage would not be to change how litigation would work — which would still be resolved under separate standards for motions to dismiss, motions for summary judgment and final resolution of litigation on the merits — but rather to spur Commissioners to demand more analytical work of the staff. Some such change is likely the only way to create sustainable analytical discipline inside the Commission.

IX. Conclusion

There is little reason to expect that the FTC will not continue to more and more closely resemble the Federal Technology Commission with each passing year: the Commission will continue to grapple with new issues. This is just as Congress intended. But if the agency is to be trusted with such broad power, Congress should expect — and indeed take steps to ensure — that the FTC does more to justify how it wields that power. As Sens. Barry Goldwater (R-AZ) & Harrison Schmitt (D-AZ) said in 1980:

> Considering that rules of the Commission may apply to any act or practice "affecting commerce", and that the only statutory restraint is that it be unfair, the apparent power of the Commission with respect to commercial law is virtually as broad as the Congress itself. In fact, the Federal Trade Commission may be the second most powerful legislature in the country…. All 50 State legislatures and State Supreme Courts can agree that a particular act is fair and lawful, but the five-man appointed FTC can overrule them all. The Congress has little control over the far-flung activities of this agency short of passing entirely new legislation.[210]

This testimony, and the attached documents, lay out some of the ideas that Congress should consider in assessing how to reform the FTC's processes and standards. But these questions are sufficiently complex, and have been simmering for long enough, that the Committee would benefit from finding ways to maximize the input of outside experts.

One model for that would be the House Energy & Commerce Committee's ongoing #CommActUpdate effort.[211] The Committee has issued six white papers, each time taking public comment and refining its proposals. Given the complex interrelationships among the pieces of FTC reform, this would be a more constructive approach than having a flurry of separate bills, as Energy & Commerce did with FTC reform.

---

[210] S. Rep. No. 96-184, at 18 (1980), available at http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=417102.

[211] The Energy and Commerce Committee, #COMMSUPDATE (last visited Sept. 25, 11:00 AM), https://energycommerce.house.gov/commactupdate/.

The Committee could also consider establishing a blue-ribbon Commission modeled on the Antitrust Modernization Commission — as TechFreedom and the International Center for Law & Economics proposed in 2014:

> A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.[212]

We stand ready to assist the Committee in whatever approach it takes.

[212] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf

The Federal Trade Commission:

Restoring Congressional Oversight of the Second National Legislature

AN ANALYSIS OF PROPOSED LEGISLATION

by Berin Szóka & Geoffrey A. Manne

May 2016

Report 2.0

FTC: Technology & Reform Project

The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature

AN ANALYSIS OF PROPOSED LEGISLATION

Berin Szóka[i] & Geoffrey A. Manne[ii]

May 2016

Report 2.0 of the FTC: Technology & Reform Project

The "FTC: Technology & Reform Project" was convened by the International Center for Law & Economics and TechFreedom in 2013. It is not affiliated in any way with the FTC.

Executive Summary

Congressional reauthorization of the FTC is long overdue. It has been twenty-two years since Congress last gave the FTC a significant course-correction and even that one, codifying the heart of the FTC's 1980 Unfairness Policy Statement, has not had the effect Congress expected. Indeed, neither that policy statement nor the 1983 Deception Policy Statement, nor the 2015 Unfair Methods of Competition Enforcement Policy Statement, will, on their own, ensure that the FTC strikes the right balance between over- and under-enforcement of its uniquely broad mandate under Section 5 of the FTC Act.

These statements are not without value, and we support codifying the other key provisions of the Unfairness Policy Statement that were not codified in 1980, as well as codifying the Deception Policy Statement. In particular, we urge Congress or the FTC to clarify the

[i] Berin Szóka is President of TechFreedom (techfreedom.org), a non-profit, tax-exempt think tank based in Washington D.C. He can be reached at bszoka@techfreedom.org or @BerinSzoka.

[ii] Geoffrey Manne is Executive Director of the International Center for Law & Economics (laweconcenter.org), a non-profit think tank based in Portland, Oregon. He can be reached at gmanne@laweconcenter.org or @GeoffManne.

meaning of "materiality," the key element of Deception, which the Commission has effectively nullified.

But a shoring up of substantive standards does not address the core problem: ultimately, that the FTC's *processes* have enabled it to operate with essentially unbounded discretion in developing the doctrine by which its three high level standards are applied in real-world cases.

Chiefly, the FTC has been able to circumvent judicial review through what it calls its "common law of consent decrees," and to effectively circumvent the rulemaking safeguards imposed by Congress in 1980 through a variety of forms of "soft law": guidance and recommendations that have, if indirectly and through amorphous forms of pressure, essentially regulatory effect.

At the same time, and contributing to the problem, the FTC has made insufficient use of its Bureau of Economics, which ought to be the agency's crown jewel: a dedicated, internal think tank of talented economists who can help steer the FTC's enforcement and policymaking functions. While BE has been well integrated into the Commission's antitrust decisionmaking, it has long resisted applying the lessons of law and economics to its consumer protection work.

The FTC is, in short, in need of a recalibration. In this paper we evaluate nine of the seventeen FTC reform bills proposed by members of the Commerce, Manufacturing and Trade Subcommittee, and suggest a number of our own, additional reforms for the agency.

Many of what we see as the most needed reforms go to the lack of economic analysis. Thus we offer detailed suggestions for how to operationalize a greater commitment to economic rigor in the agency's decision-making at all stages. Specifically, we propose expanding the proposed requirement for economic analysis of recommendations for "legislation or regulatory action" to include best practices (such as the FTC commonly recommends in reports), complaints and consent decrees. We also propose (and support bills proposing) other mechanisms aimed at injecting more rigor into the Commission's decisionmaking, particularly by limiting its use of various sources of informal or overly discretionary sources of authority.

The most underappreciated aspect of the FTC's processes is investigation, for it is here that the FTC wields incredible power to coerce companies into settling lawsuits rather than litigating them. Requiring that the staff satisfy a "preponderance of the evidence" standard for issuing consumer protection complaints would help, on the margin, to embolden some defendants not to settle. Other proposed limits on the aggressive use of remedies and on the allowable scope of the Commission's consent orders would help to accomplish the same thing. Changing this dynamic even slightly could produce a significant shift in the agency's model, by injecting more judicial review into the FTC's evolution of its doctrine.

Commissioners themselves could play a greater role in constraining the FTC's discretion, as well, keeping the FTC focused on advancing consumer welfare in everything it does. To-

gether with the Bureau of Economics, these two internal sources of constraint could partly substitute for the relative lack of external constraint from the courts.

We are not wholly critical of the FTC. Indeed, we are broadly supportive of its mission. And we support several measures to *expand* the FTC's jurisdiction to cover telecom common carriers and to make it easier for the FTC to prosecute non-profits that engage in for-profit activities. We enthusiastically support expansion of the FTC's Bureau of Economics. And we recommend expansion of the Commission's competition advocacy work into a full-fledged Bureau, so that the Commission can advocate at all levels of government — federal, state and local — on behalf of consumers and against legislation and regulations that would hamper the innovation and experimentation that fuel our rapidly evolving economy.

But most of all, Congress should not take the FTC's current processes for granted. Ultimately, the FTC reports to Congress and it is Congress's responsibility to regularly and carefully scrutinize how the agency operates. The agency's vague standards, sweeping jurisdiction, and its demonstrated ability to circumvent both judicial review and statutory safeguards on policy making make regular reassessment of the Commission through biennial reauthorization crucial to its ability to serve the consumers it is tasked with protecting.

Table of Contents

> Considering that rules of the Commission may apply to any act or practice "affecting commerce", and that the only statutory restraint is that it be unfair, **the apparent power of the Commission with respect to commercial law is virtually as broad as the Congress itself. In fact, the Federal Trade Commission may be the second most powerful legislature in the country….** All 50 State legislatures and State Supreme Courts can agree that a particular act is fair and lawful, but the five-man appointed FTC can overrule them all. **The Congress has little control over the far-flung activities of this agency short of passing entirely new legislation**.[1]
>
> *Sens. Barry Goldwater & Harrison Schmitt, 1980*

> **Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been "lawless" in the sense that it has traditionally been beyond judicial control**.[2]
>
> *Former FTC Chairman Tim Muris, 1981*

> **The FTC's investigatory power is very broad and is akin to an inquisitorial body.** On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[3]
>
> *Prof. Chris Hoofnagle, 2016*

Introduction

Only by the skin of its teeth did the Federal Trade Commission survive its cataclysmic confrontation with Congress in 1980. Today, the Federal Trade Commission remains the closest thing to a second national legislature in America. Its jurisdiction covers nearly every company in America. It powers over unfair and deceptive acts and practices (UDAP) and unfair methods of competition (UMC) remain so inherently vague that the Commission retains unparalleled discretion to make policy decisions that are essentially legislative. The Commission increasingly wields these powers over high tech issues affecting not just the high tech *sector*, but, increasingly, every company in America. It has become the de facto

---

[1] S. Rep. No. 96-184, at 18 (1980), *available at* http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=417102.

[2] Timothy J. Muris, *Judicial Constraints*, in THE FEDERAL TRADE COMMISSION SINCE 1970: ECONOMIC REGULATION AND BUREAUCRATIC BEHAVIOR, 35, 49 (Kenneth W. Clarkson & Timothy J. Muris, eds., 1981).

[3] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY 102 (2016).

Federal *Technology* Commission — a moniker we coined,[4] but which Chairwoman Edith Ramirez has embraced.[5]

For all this power, either by design or by neglect, the FTC is also "a largely unconstrained agency."[6] "Although appearing effective, most means of controlling Commission actions are virtually useless, owing to lack of political support and information, lack of interest on the part of those ostensibly monitoring the FTC, or FTC maneuvering."[7] At the same time, "[t]he courts place almost no restraint upon what commercial practices the FTC can proscribe…."[8]

The vast majority of what the FTC does is uncontroversial — routine antitrust, fraud and advertising cases. Yet, as the FTC has dealt with cutting-edge legal issues, like privacy, data security and product design, it has raised deep concerns not merely about the specific cases brought by the FTC, but also that the agency is drifting away from the careful balance it struck in its 1980 Unfairness Policy Statement (UPS)[9] and its 1983 Deception Policy Statement (DPS).[10]

We applaud the Commerce, Manufacturing & Trade Subcommittee for taking up the issue of FTC reform, and for the seventeen bills submitted by members of both parties. Even if no legislation passes this Congress, active engagement by Congress in the operation of the Commission was crucial in the past to ensuring that the FTC does not stray from its mission of serving consumers. But active congressional oversight has been wanting for far too long.

---

[4] Berin Szóka & Geoffrey Manne, *The Second Century of the Federal Trade Commission*, TECHDIRT (Sept. 26, 2013), *available at* https://www.techdirt.com/blog/innovation/articles/20130926/16542624670/second-century-federal-trade-commission.shtml*; see also Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission*, Report 1.0 of the FTC: Technology & Reform Project, 3 (Dec. 2013), *available at* http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[5] Kai Ryssdal, *The FTC is Dealing with More High Tech Issues*, MARKETPLACE (Mar. 7, 2016), *available at* http://www.marketplace.org/2016/03/07/tech/ftc-dealing-more-high-tech-issues.

[6] *Part I: The Institutional Setting*, in THE FEDERAL TRADE COMMISSION SINCE 1970, *supra* note 2 at 11.

[7] *Id*. at 11–12.

[8] Timothy J. Muris, *Judicial Constraints*, in *id*. 35, 43.

[9] *Letter from the FTC to the House Consumer Subcommittee, appended to* In re Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984) ["Unfairness Policy Statement" or "UPS"], *available at* http://www.ftc.gov/ftc-policy-statement-on-unfairness.

[10] *Letter from the FTC to the Committee on Energy & Commerce, appended to* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984) ["Deception Policy Statement" or "DPS"], *available at* http://www.ftc.gov/ftc-policy-statement-on-deception.

Not since 1996 has Congress reauthorized the FTC,[11] and not since 1994 has Congress actually substantially modified the FTC's standards or processes.[12]

The most significant thing Congress has done regarding the FTC since 1980 was the 1994 codification of the Unfairness Policy Statement's three-part balancing test in Section 5(n). But even that has proven relatively ineffective: The Commission pays lip service to this test, but there has been essentially none of analytical development promised by the Commission in the 1980 UPS:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, **subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time**.

The Commission no doubt believes that it has carefully weighed (1) substantial consumer injury with (2) countervailing benefit to consumers or to competition, and carefully assessed whether (3) consumers could "reasonably have avoided" the injury, as Congress required by enacting Section 5(n). But whatever weighing the Commission has done in its internal decision-making is far from apparent from the outside, and it has not been done by the courts in any meaningful way.[13] As former Chairman Tim Muris notes, "the Commission's authority remains extremely broad."[14]

The situation is little on better on Deception — at least, on the cutting edge of Deception cases, involving privacy policies, online help pages, and enforcement of other promises that differ fundamentally from traditional marketing claims. Just as the Commission has rendered the three-part Unfairness test essentially meaningless, it has essentially nullified the "materiality" requirement that it volunteered in the 1983 Deception Policy Statement. The Statement began by presuming, reasonably, that express *marketing* claims are always materi-

---

[11] Federal Trade Commission Reauthorization Act of 1996, Pub. L. 104-216, 110 Stat. 3019 (Oct. 1, 1996), *available at* http://uscode.house.gov/statutes/pl/104/216.pdf.

[12] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691 (Aug. 26, 1994) *available at* http://uscode.house.gov/statutes/pl/103/312.pdf.

[13] *See infra* at 39.

[14] Statement of Timothy J. Muris, Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation, 111th Cong. 2 (2010), 28, *available at* http://lawprofessors.typepad.com/files/muris_senate_testimony_ftc_role_protecting_consumers_3-17-101.pdf.

al, but the Commission has extended that presumption (and other narrow presumptions of materiality in the DPS) to cover essentially *all* deception cases.[15]

Congress cannot fix these problems simply by telling the FTC to dust off its two bedrock policy statements and take them more seriously (as it essentially did in 1994 regarding Unfairness). Instead, Congress must fundamentally reassess the *process* that has allowed the FTC to avoid judicial scrutiny of how it wields its discretion.

The last time Congress significantly reassessed the FTC's *processes* was in May 1980, when it created procedural safeguards and evidentiary requirements for FTC rulemaking. These reforms were much needed, and remain fundamentally necessary (although we do, below, encourage the FTC to attempt a Section 5 rulemaking for the first time in decades in order to provide a real-world experience of how such rulemakings work and whether Congress might make changes at the margins to facilitate reliance on that tool).[16]

But these 1980 reforms failed to envision that the Commission would, eventually, find ways of exercising the vast discretion inherent in Unfairness and Deception through what it now proudly calls its "common law of consent decrees"[17] — company-specific, but cookie-cutter consent decrees that have little to do with the facts of each case (and always run for twenty years). These consent decrees are bolstered by the regular issuance of recommended best practices in reports and guides that function as quasi-regulations, imposed on entire industries not by rulemaking but by the administrative equivalent of a leering glare. Together, these new tactics have allowed the FTC to effectively circumvent not only the process re-

---

[15] *See infra* at 21.

[16] *See infra* at 99.

[17] "Together, these enforcement efforts have established what some scholars call 'the common law of privacy' in the United States." Julie Brill, Commissioner, Fed. Trade Comm'n, *Remarks to the Mentor Group Forum for EU-US Legal-Economic Affairs Brussels, April 16, 2013*, 3 (Apr. 16, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-mentor-group-forum-eu-us-legal-economic-affairs-brussels-belgium/130416mentorgroup.pdf (citing Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States* (2010), *available at* http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8- 4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow.")). FTC Chairman Edith Ramirez said roughly the same thing in a 2014 speech:

> I have expressed concern about recent proposals to formulate guidance to try to codify our unfair methods principles for the first time in the Commission's 100 year history. While I don't object to guidance in theory, I am less interested in prescribing our future enforcement actions than in describing our broad enforcement principles revealed in our recent precedent.

Quoted in Geoffrey Manne, *FTC Commissioner Joshua Wright gets his competition enforcement guidelines*, TRUTH ON THE MARKET (Aug. 13, 2015), *available at* https://truthonthemarket.com/2015/08/13/ftc-commissioner-joshua-wright-gets-his-competiton-enforcement-guidelines/ (*speech video available at* http://masonlec.org/media-center/299).

forms of May 1980 but also the substantive constraints volunteered by the FTC later that year in the Unfairness Policy Statement and, three years later, in the Deception Policy Statement.

Such process reforms are the focus of this paper. The seventeen bills currently before the Subcommittee would begin to address these problems — but only begin. In this paper we evaluate nine of the proposed bills in turn, offer specific recommendations, and also offer a slate of our own additional suggestions for reform.

Our most important point, though, is not any one of our proposed reforms, but this: The default assumption should not be that the FTC continues operating indefinitely without course corrections from Congress.

Justice Scalia put this point best in his 2014 decision, striking down the EPA's attempt to "rewrite clear statutory terms to suit its own sense of how the statute should operate," when he said: "We are not willing to stand on the dock and wave goodbye as EPA embarks on this multiyear voyage of discovery."[18] The point is more, not less, important when a statute like Section 5 has been "deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion": trusting the FTC to follow an "evolutionary process" *requires* regular, searching reassessments by Congress. This need is especially acute given that the "underlying criteria" have *not* "evolve[d] and develop[ed] over time" through the "judicial review" expected by both Congress and the FTC in 1980 — at least, not in any analytically meaningful way.

Reauthorization should happen at regular two-year intervals and it should never be a *pro forma* rubber-stamping of the FTC's processes. Each reauthorization should begin from the assumption that the FTC is a uniquely important and valuable agency — one that can do enormous good for consumers, but also one whose uniquely broad scope and broad discretion require constant supervision and regular course corrections. Regular tweaks to the FTC's processes should be expected and welcomed, not resisted.

The worst thing defenders of the FTC could do would be allowing the FTC to drift along towards the kind of confrontation with Congress that nearly destroyed the FTC in 1980.

The FTC's History: Past is Prologue

It is no exaggeration to say that the 1980 compromise over unfairness saved the FTC from going the way of the Civil Aeronautics Board, which Congress began phasing out in 1978 under the leadership of Alfred Kahn, President Carter's de-regulator-in-chief. President

[18] Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2446 (2014).

Carter signed the 1980 FTC Improvements Act even though he objected to some of its provisions because, as he noted, "the very existence of this agency is at stake."[19] Those reforms to the FTC's rulemaking process, enacted in May 1980, were only part of what saved the FTC from oblivion.

Driven largely by outrage over the FTC's attempt to regulate children's advertising, Congress had allowed the FTC's funding to lapse, briefly shuttering the FTC. As Howard Beales, then (in 2004) director of the FTC's Bureau of Consumer Protection, noted, "shutting down a single agency because of disputes over policy decisions is almost unprecedented."[20] In the mid-to-late 1970s, the FTC had interpreted "unfairness" expansively in an attempt to regulate everything from funeral home practices to labor practices and pollution. Beales and former FTC Chairman, Tim Muris, summarize the problem thusly:

> Using its unfairness authority under Section 5, but unbounded by meaningful standards, in the 1970s the Commission embarked on a vast enterprise to transform entire industries. Over a 15-month period, the Commission issued a rule a month, usually without a clear theory of why there was a law violation, with only a tenuous connection between the perceived problem and the recommended remedy, and with, at best, a shaky empirical foundation.[21]

When the FTC attempted to ban the advertising of sugared cereals to children, the Washington Post dubbed the FTC the "National Nanny."[22] This led directly to the 1980 FTC Improvements Act — the one Sens. Goldwater and Schmitt endorsed in the quotation that opens this paper.

In early 1980, by a vote of 272-127, Congress curtailed the FTC's Section 5 rulemaking powers under the 1975 Magnuson-Moss Act, imposing additional evidentiary and procedural safeguards.[23] But the FTC refused to narrow its doctrinal interpretation of unfairness until Congress briefly shuttered the FTC in the first modern government shutdown. In December, 1980, the FTC issued its Unfairness Policy Statement, promising to weigh (a) sub-

---

[19] Jimmy Carter, *Federal Trade Commission Improvements Act of 1980 Statement on Signing H.R. 2313 into Law* (May 28, 1980), *available at* http://www.presidency.ucsb.edu/ws/?pid=44790.

[20] J. Howard Beales III, *Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present*, 8 n.32 (2004), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kids-and-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf.

[21] J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(B) of the FTC Act*, 79 ANTITRUST L. J. 1, 1 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764456.

[22] Editorial, WASH. POST (Mar. 1, 1978), reprinted in MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION, 69–70 (1982); *see also* Beales, *supra* note 20, at 8 n.37 ("Former FTC Chairman Pertschuk characterizes the Post editorial as a turning point in the Federal Trade Commission's fortunes.").

[23] Federal Trade Commission Act Improvements Act of 1980, Pub. L. 96-252, 94 Stat. 374 (May 28, 1980), *available at* http://uscode.house.gov/statutes/pl/96/252.pdf.

stantial injury against (b) countervailing benefit and (c) to focus only on practices consumers could not reasonably avoid. Last year, the FTC finally adopted a Policy Statement on Unfair Methods of Competition that parallels the two UDAP statements.[24]

In 1994, in Section 5(n), Congress codified the core requirements of the UPS, and further narrowed the FTC's ability to rely on its assertions of what constituted public policy. This was the last time Congress substantially modified the FTC Act — meaning that the Commission has operated since then without course-correction from Congress.[25] This is itself troubling, given that independent agencies are supposed to operate as creatures of Congress, not regulatory knights errant. But it is even more problematic given the extent of the FTC's renewed efforts to escape the bounds of even its minimal discretionary constraints.

The Inevitable Tendency Towards the Discretionary Model

To paraphrase Winston Churchill on democracy, the FTC offers the "worst form of consumer protection and competition regulation — except for all the others." Democracy, without constant vigilance and reform, will inevitably morph into the unaccountable exercise of power — what the Founders meant by the word "corruption" (literally, "decayed"). When Benjamin Franklin was asked, upon exiting the Constitutional Convention of 1787, "Well, Doctor, what have we got — a Republic or a Monarchy?," he famously remarked "A Republic, if you can keep it."[26]

The same can be said for the FTC: an "evolutionary process… subject to judicial review,"[27] *if we can keep it*. Any agency given so broad a charge as to prohibit "unfair methods of competition… and unfair or deceptive acts or practices…" will inevitably tend towards the exercise of maximum discretion.

This critique is of a dynamic inherent in the FTC itself, not of particular Chairmen, Commissioners, Bureau Directors or other staffers. The players change regularly, each leaving their mark on the agency, but the agency has institutional tendencies of its own, inherent in the nature of the agency.

The Commission itself most clearly identified the core of the FTC's institutional nature in the Unfairness Policy Statement, in a passage so critical it bears quoting in full:

---

[24] Fed. Trade Comm'n, *Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act* (Aug. 13, 2015) ["UMC Policy Statement"], *available at* https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

[25] The 1996 FTC reauthorization was purely *pro forma*.

[26] Benjamin Franklin, *quoted in* Respectfully Quoted: A Dictionary of Quotations, BARTLEBY.COM (last visited May 22, 2016), http://www.bartleby.com/73/1593.html

[27] UPS, *supra* note 9.

> The **present understanding of the unfairness standard is the result of an evolutionary process**. The **statute was deliberately framed in general terms** since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in **the expectation that the underlying criteria would evolve and develop over time**. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the **gradual process of judicial inclusion and exclusion**.'"[28]

In other words, Congress delegated vast discretion to the Commission from the very start because of the difficulties inherent in prescriptive regulation of competition and consumer protection. The Commission generally exercised that discretion primarily through case-by-case adjudication, but began issuing rules on its own authority in 1964,[29] setting it on the road that culminated in the cataclysm of 1980.

Indeed, given the essential nature of bureaucracies, it was probably only a matter of time before the FTC reached this point. It is no accident that it took just three years from 1975, when Congress affirmed the FTC's claims to "organic" rulemaking power (implicit in Section 5), until the FTC was being ridiculed as the "National Nanny." In short, the 1975 Magnuson-Moss Act created a monster, magnifying the effects of the FTC's inherent Section 5 discretion with the ability to conduct statutorily sanctioned rulemakings. If it had not been then-Chairman Michael Pertschuk who pushed the FTC too far, it probably would have, eventually, been some other chairman. The power was simply too great for any government agency to resist using without some feedback mechanism in the system telling it to stop.

In that sense, we believe the rise of the Internet played a role analogous to the 1975 Magnuson-Moss Act, spurring the FTC to greater activity where it had previously been more restrained.[30]

After 1980, the FTC ceased conducting new Section 5 rulemakings. Between 1980 and 2000, the FTC brought just sixteen unfairness cases, all of which fell into narrow categories of clearly "bad" conduct: "(1) theft and the facilitation thereof (clearly the leading category);

---

[28] UPS, *supra* note 9.

[29] Statement of Basis and Purpose, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (1964).

[30] Of course, we also recognize that other societal forces were at work, such as the Naderite consumer protection movement of the 1970s, and the growing privacy protection movement of the 1990s and 2000s. But the analogy still offers some value.

(2) breaking or causing the breaking of other laws; (3) using insufficient care; (4) interfering with the exercise of consumer rights; and (5) advertising that promotes unsafe practices."[31] Just how easy these cases were conveys in turn just how *cautious* the Commission was in using its unfairness powers — not only because it was chastened by the experience of 1980 but also because of Congress's reaffirmation of the limits on unfairness in its 1994 codification of Section 5(n). In a 2000 speech, Commissioner Leary summarized the Commission's restrained, "gap-filling" approach to unfairness enforcement over the preceding two decades:

> The overall impression left by this body of law is hardly that policy has been created from whole cloth. Rather, the Commission has sought through its unfairness authority to challenge commercial conduct that under any definition would be considered wrong but which escaped or evaded prosecution by other means.[32]

Yet even then Commissioner Leary noted his concerns about the burgeoning unfairness enforcement innovation in two of the Commission's then-recent cases: *Touch Tone* (1999)[33] and ReverseAuction (2000). Tellingly, his concern was over the Commission's failure to properly assess the substantiality of the amorphous privacy injuries alleged in those cases. Still, he concluded on a note of optimism:

> The extent of the disagreement should not be exaggerated, however. The majority [in *Reverse Auction*] did not suggest that all privacy infractions are sufficiently serious to be unfair and the minority did not suggest that none of them are. The boundaries of unfairness, as applied to Internet privacy violations, remain an open question.
>
> The Commission has so far used its unfairness authority in relatively few cases that involve the Internet. These cases, however, suggest that future application of unfairness will be entirely consistent with recent history. Internet technology is new, but we have addressed new technology before. I believe that the Commission will do what it can to prevent the Internet from becoming a lawless frontier, but it will also continue to avoid excesses of paternalism.
>
> The lessons of the past continue to be relevant because the basic patterns of dishonest behavior continue to be the same. Human beings evolve much more slowly than their artifacts.[34]

---

[31] Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1962 (2000).

[32] Thomas B. Leary, Former Commissioner of the Fed. Trade Comm'n, *Unfairness and the Internet*, II (Apr. 13, 2000), *available at* http://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

[33] *Id.* at II-C ("The unfairness count in Touch Tone also raised interesting questions about whether an invasion of privacy by itself meets the statutory requirement that unfairness cause "substantial injury." Unlike most unfairness prosecutions, there was no concrete monetary harm or obvious and immediate safety or health risks. The defendants' revenue came, not from defrauding consumers, but from the purchasers of the information who received exactly what they had requested.").

[34] *Id.*, at III-IV.

The Commission began bringing cases in 2000 alleging that companies employed unreasonable data security practices. While these early cases alleged that the practices were "unfair *and* deceptive," they were, in fact, pure deception cases.[35] In 2005, the FTC filed its first pure unfairness data security action, against BJ's Warehouse. Unlike past defendants, BJ's had, apparently, made no promise regarding data security upon which the FTC could have hung a deception action.[36] Since 2009, we believe the Commission has become considerably more aggressive in its prosecution of unfairness cases, not just about data security, but about privacy and other high tech issues like product design.

Yet it would be hard to pinpoint a single moment when the FTC's approach changed, or to draw a clear line between Republican data security cases and Democratic ones. And this is precisely a function of the first of the two crucial attributes of the modern FTC with which we are concerned: Legal doctrine continues to evolve even in the absence of judicial decisions, its evolution just becomes less transparent and more amorphous. As Commissioner Leary remarked in a footnote that now seems prescient:

> Because this case was settled, I cannot be sure that the other Commissioners agreed with this rationale.[37]

Indeed, this is the crucial difference between the FTC's pseudo common law and *real* common law. There is an observable directedness to the evolution of the real common law, which rests on a sort of ongoing conversation among the courts and the economic actors that appear before them. The FTC's ersatz common law, however, has little of this directedness or openness, and the conversations that do occur are more like whispered tête-à-têtes in the corner that someone else occasionally overhears.

But the second point is actually the more important, although the two are related: In this institutional structure, how often individual Commissioners dissent and how much rigor they demand matters far, far less than the structure of the agency itself. There is only so much an individual can do to divert the path of an already-steaming ship.

This leads back to the point made above: that we should expect regulatory agencies, over time, to expand their discretion as much as the constraints upon the agency allow. In this, regulatory agencies resemble gases, which, when unconstrained, do not occupy a fixed volume (defined by a clear statutory scheme, as in the Rulemaking Model) but rather expand to

---

[35] See, e.g., FTC v. Rennert, Complaint, FTC File No. 992 3245, http://www.ftc.gov/os/2000/07/iogcomp.htm (2000); In re Eli Lilly, Complaint, File No. 012 3214, http://www.ftc.gov/os/2002/05/elilillycmp.htm (2002).

[36] Complaint, In the Matter of BJ's Wholesale Club, Inc., a corporation, Fed. Trade Comm'n Docket No. C-4148, *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

[37] Leary, *Unfairness and the Internet*, *supra* note 32, n.50.

fill whatever space they occupy. What ultimately determines the size, volume and shape of a gas is its container. So, too, with regulatory agencies: what ultimately determines an agency's scale, scope, and agenda are the external constraints that operate upon it.

The FTC has evolved the way it has because, most fundamentally, Section 5 offers little in the way of prescriptive, statutory constraints, and because the FTC's processes have enabled it to operate case-by-case with relatively little meaningful, ongoing oversight from the courts.

We distinguish this from two other models of regulation: (1) the **Rulemaking Model**, in which the agency's discretion is constrained chiefly by the language of its organic statute, procedural rulemaking requirements and the courts; and (2) the **Evolutionary Model**, in which the agency applies a vague standard case by case, but is constrained in doing so by its ongoing interaction with the courts.[38] By contrast, we call the FTC's current approach the **Discretionary Model**, in which the agency also applies a vague standard case-by-case, but in which it operates without meaningful judicial oversight, such that doctrine evolves at the Commission's discretion and with little of the transparency provided by published judicial opinions. (Dialogue between majority and minority Commissioners seldom approaches the analysis of judicial opinions.)

We believe there is an inherent tendency of agencies that begin with an Evolutionary Model — which is very much the design of the FTC — to slide towards the Discretionary Model, simply because all agencies tend to maximize their own discretion, and because the freedom afforded by the lack of statutory constraints on substance or the agency's case-by-case process enable these agencies to further evade judicial constraints. The only way to check this process, without, of course, simply circumscribing its discretion by substantive statute (i.e., amending section 5(a)(2)), is regular assessment and course-correction by Congress — not with the aim of its own micromanagement of the agency, but rather with the aim of invigorating the ability of the courts to exert their essential role in steering doctrine.

This is not to be taken as an admission of defeat or a condemnation of the Commission. There is no reason to think that the FTC was in every way ideally constituted from the start (or in 1980 or in 1994), that its model could perform exactly as intended and perfectly in the public interest no matter what changed around it. Rather, limited, thoughtful oversight by

---

[38] We derive the term "evolutionary" from the Unfairness Policy Statement itself, *supra* note 9:

> *The present understanding of the unfairness standard is the result of an evolutionary process*. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time.

Congress is simply in the nature of the beast. As Justice Holmes said (of the importance of free speech):

> That, at any rate, is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year, if not every day, we have to wager our salvation upon some prophecy based upon imperfect knowledge.[39]

That, in a nutshell, is why regular reauthorization is critical for agencies like the FTC. As President Carter said, "[w]e need vigorous congressional oversight of regulatory agencies." This is more true for the FTC — with its vast discretion, immense investigative power, and all-encompassing scope — than any other agency. As we wrote in the precursor to this report:

> Thus, while the Congress of 1914 intended to create an agency better suited than itself to establish a flexible but predictable and consistent body of law governing commercial conduct, the modern trend of administrative law has relaxed the requirement that an agency's output be predictable or consistent.
>
> The FTC has embraced this flexibility as few other agencies have. Particularly in its efforts to keep pace with changing technology, the FTC has embraced its role as an administrative agency, and frequently sought to untether itself from ordinary principles of jurisprudence (let alone judicial review).[40]

The Doctrinal Pyramid

One of the chief reasons the FTC has come to operate the way it does is that the vocabulary around its operations is deeply confused, particularly around the word "guidance" and the term "common law." In an (admittedly first-cut) effort to introduce some concreteness, we view the various levels of "guidance" as steps in a Doctrinal Pyramid that looks something like the following, from highest to lowest degrees of authority:

1. **The Statute**: Section 5 (and other, issue-specific statutes)
2. **Litigated Cases**: Only these are technically binding on courts, thus they rank near the top of the pyramid, even though they are synthesized in, or cited by, the guidance summarized below. There are precious few of these on Unfairness or the key emerging issues of Deception
3. **Litigated Preliminary Injunctions**: Less meaningful than full adjudications of Section 5, these are, unfortunately, largely the only judicial opinions on Section 5.
4. **High-Level Policy Statements**: Unfairness, Deception, Unfair Methods of Competition

---

[39] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting).

[40] *Consumer Protection & Competition Regulation in a High-Tech World, supra*, note 4.

5. **Lower-Level Policy Statements**: The now-rescinded Disgorgement Policy Statement, the (not-yet existent) Materiality Statement we propose, *etc.*
6. **Guidelines**: Akin to the several DOJ/FTC Antitrust Guidelines, synthesizing past approaches to enforcement into discernible principles to guide future enforcement and compliance
7. **Consent Decrees**: Not binding upon the Commission and hinging (indirectly) upon the very low bar of whether the Commission has "reason to believe" a violation occurred, these provide little guidance as to how the FTC really understands Section 5
8. **Closing Letters**: Issued by the staff, these letters at times provide some limited guidance as to what the staff believe is *not* illegal
9. **Reports & Recommendations**: In their current form, the FTC's reports do little more than offer the majority's views of what companies should do to comply with Section 5, but carefully avoid any real legal analysis
10. **Industry Guides**: Issue-specific discussions issued by staff (*e.g.*, photo copier data security)
11. **Public Pronouncements**: Blog posts, press releases, congressional testimony, FAQs, etc.

In essence, under today's Discretionary Model, the FTC puts great weight on the base of the pyramid, while doing little to develop the top. Under the Evolutionary Model, the full Commission would develop doctrine primarily through litigation, and do everything it possibly could to provide guidance at higher levels of the pyramid, such as by debating, refining and voting upon new Policy Statements on each of the component elements of Unfairness and Deception and Guidelines akin to the Horizontal Merger Guidelines. Instead, the FTC staff issues Guides and other forms of casual guidance. Yet not all "guidance" is of equal value. Indeed, much of the "guidance" issued by the FTC serves not to constrain its discretion, but rather to expand it by increasing the agency's ability to coerce private parties into settlements — which begins the cycle anew.

Our Proposed Reforms

Seventeen bills have been introduced in the House Energy & Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade aimed at reforming the agency for the modern, technological age and improving FTC process and subject-matter scope in order to better protect consumers. Most of these will, we hope, be consolidated into a single FTC Reauthorization Act of 2016, passed in both chambers, and signed by the President.

With the hope of aiding this process, we describe and assess nine of these proposed bills, focusing in particular on whether and how well each proposal addresses the fundamental issues that define the problems of today's FTC. In broad strokes, the proposed bills address the following areas:

- Substantive standards
- Enforcement and guidance
- Remedies

- Other process issues
- Jurisdictional issues
- Other issues

Our analysis addresses the bills within the context of these broad categories, and adds our own suggestions (and one additional category: Competition Advocacy) for both minor amendments and additional legislation in each category.

Despite our concerns, we remain broadly supportive of the FTC's mission and we generally support expanding the agency's jurisdiction, to the extent that doing so effectively addresses substantial, identifiable consumer harms or reduces the scope of authority for sector-specific agencies. Although the process reforms proposed in these bills are, we believe, relatively minor, targeted adjustments, taken together they would do much to make the FTC more effective in its core mission of maximizing consumer welfare. But these proposed reforms are only a beginning.

Even if all of these reforms were enacted immediately, they would not fundamentally, or even substantially, change the core functioning of the FTC — and the core problem at the FTC today: its largely unconstrained discretion.

The FTC loudly proclaims the advantages of its *ex post* approach of relying on case-by-case enforcement of UDAP and UMC standards rather than rigid *ex ante* rulemaking, especially over cutting-edge issues of consumer protection. And there is much to commend this sort of approach relative to the prescriptive regulatory paradigm that characterizes many other agencies — again, the Evolutionary Model. But under the FTC's *Discretionary* Model, the Commission uses its "common law of consent decrees" (more than a hundred high-tech cases settled without adjudication, and with essentially zero litigated cases to guide these settlements) and a mix of other forms of soft law (increasingly prescriptive reports based on workshops tailored to produce predetermined outcomes, and various other public pronouncements), to "regulate" — or, more accurately, to try to steer — the evolution of technology.

The required balancing of tradeoffs inherent in unfairness and deception have little meaning if the courts do not review, follow or enforce them; if the Bureau of Economics has little role in the evaluation of these inherently economic considerations embodied in the enforcement decision-making of the Bureau of Consumer Protection or in its workshops; and if other Commissioners are able only to quibble on the margins about the decisions made by the FTC Chairman. Simply codifying these standards, as Congress codified the heart of the Unfairness Policy Statement in Section 45(n) back in 1994, and as the proposed CLEAR Act would finish doing, will not solve the problem: The FTC has routinely circumvented the rigorous analysis demanded by these standards, and the same processes would enable it to continue doing so.

To address these concerns, we also propose here a number of further process reforms that we believe would begin to correct these problems and ensure that the Commission's process really does serve the consumers the agency was tasked with protecting.

Our aim is not to hamstring the Commission, but to ensure that it wields its mighty powers with greater analytical rigor — something that should inure significantly to the benefit of consumers. Ideally, the impetus for such rigor would be provided by the courts, through careful weighing of the FTC's implementation of substantive standards in at least a small-but-significant percentage of cases. Those decisions would, in turn, shape the FTC's exercise of its discretion in the vast majority of cases that will — and should, in such an environment — inevitably settle out of court. The Bureau of Economics and the other Commissioners would also have far larger roles in ensuring that the FTC takes its standards seriously. But reaching these outcomes requires adjustment to the Commission's *processes*, not merely further codification of the standards the agency already purports to follow.

We believe that our reforms should attract wide bipartisan support, if properly understood, and that they would put the FTC on sound footing for its second century — one that will increasingly see the FTC assert itself as the Federal Technology Commission.

FTC Act Statutory Standards

Unfairness

The Statement on Unfairness Reinforcement & Emphasis (SURE) Act

Rep. Markwayne Mullin's (R-OK) bill (H.R. 5115)[41] further codifies promises the FTC made in its 1980 Unfairness Policy Statement — thus picking up where Congress left off in 1994, the last time Congress reauthorized the FTC in Section 5(n):

> The Commission shall have no authority … to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice [i] causes or is likely to cause substantial injury to consumers [ii] which is not reasonably avoidable by consumers themselves and [iii] not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[42]

[41] The Statement on Unfairness Reinforcement and Emphasis Act, H.R. 5115,114th Cong. (2016) [hereinafter SURE Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5115/text.

[42] 15 U.S.C. § 45(n).

This effectively codified the core of the Unfairness Policy Statement, while barring the FTC from relying on public policy determinations alone.[43] The bill would add several additional clauses to Section 5(n), drawn from the Unfairness Policy Statement. Most importantly:

1. It would exclude "trivial or merely speculative" harm from the definition of "substantial" injury.[44]
2. It would enhance the Act's "countervailing benefits" language to require consideration of the "net effects" of conduct, including dynamic, indirect consequences (like effects on innovation).[45]
3. It would prohibit the Commission from "second-guess[ing] the wisdom of particular consumer decisions," and encourage it to ensure "the free exercise of consumer decisionmaking."[46]

These provisions in particular (along with the others included in the bill, to be sure) would codify core aspects of the economic trade-off embodied in the UPS. They would enhance the Commission's administrative efficiency and direct its resources where consumers are most benefited. They would ensure that the FTC's weighing of costs and benefits is as comprehensive as possible, avoiding the systematic focus on concrete, short-term costs to the exclusion of larger, longer-term benefits. And they would help to preserve the inherent benefits of consumer choice, and avoid the intrinsic costs of agency paternalism.

Codification of these provisions would benefit consumers. And because H.R. 5115's language hews almost verbatim to the Unfairness Policy Statement, it should be uncontroversial. Effectively, it simply makes binding those parts of the UPS that Congress did not codify back in 1994.

---

[43] The Unfairness Policy Statement had said:

> Sometimes public policy will independently support a Commission action. This occurs when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission….
>
> To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values. The policy should likewise be one that is widely shared, and not the isolated decision of a single state or a single court. If these two tests are not met the policy cannot be considered as an "established" public policy for purposes of the S&H criterion. The Commission would then act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury.

UPS, *supra* note 9.

[44] SURE Act, *supra* note 41.

[45] *Id.*

[46] *Id.*

VALUE OF THE BILL: Codifying the Unfairness Policy Statement Would Reaffirm its Value, Encouraging Dissents and Litigation

Codifying a policy statement, even if verbatim and only in part, does essentially four things:

1. Legally, it makes the policy binding upon the Commission, since Policy Statements, technically, are not. On the margin this should deter the FTC from bringing more-tenuous cases that may not benefit consumers but that it might otherwise have brought.
2. Practically, it confers greater weight on the codified text in the Commission's deliberations, empowering dissenting Commissioners to point to the fact that Congress has chosen to codify certain language and requiring the majority to respond.
3. Legally, it somewhat reduces the deference the courts will give the FTC when it applies the statute (under *Chevron*) relative to the stronger deference given to agencies applying their own policy statements (under *Auer*).[47]
4. Perhaps most importantly, it gives defendants a stronger leg to stand on in court, thus increasing, on the margin, the number that will actually litigate rather than settle. That, in turn, benefits everyone by increasing the stock of judicial analysis of doctrine.

In all four respects, the FTC would greatly benefit from the H.R. 5115's further codification of the Unfairness Policy Statement. As a string of dissenting statements by former Commissioner Wright make lays bare, the FTC is not consistently taking the Unfairness Policy Statement seriously.[48] At most, it pays lip service even to the three core elements of unfairness set forth in Section 5(n) — and even less regard to those aspects of the UPS not codified in Section 5(n).[49]

Indeed, it is difficult to imagine any principled objection to codifying a document that the FTC already claims to observe carefully. And if the agency plans to bring unfairness cases that are *not* covered by the four corners of the Unfairness Policy Statement (yet somehow within Section 5(n)), that should be a matter of grave concern to Congress.

---

[47] Note that not everyone agrees that *Chevron* deference is weaker than *Auer* deference. *See* Sasha Volokh, *Auer and Chevron*, THE VOLOKH CONSPIRACY (Mar. 22, 2013), *available at* http://volokh.com/2013/03/22/auer-and-chevron/.

[48] *See, e.g.*, Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108 (Jan. 15, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf. *See also* Berin Szóka, *Josh Wright's Unfinished Legacy: Reforming FTC Consumer Protection Enforcement*, TRUTH ON THE MARKET (Aug. 26, 2015), https://truthonthemarket.com/2015/08/26/josh-wrights-unfinished-legacy/.

[49] UPS, *supra* note 9.

RECOMMENDATION: Require a Preponderance of the Evidence Standard for Unfairness Complaints

As valuable as codification of the substantive standards of the Unfairness Policy Statement would be, mere codification, or even tweaking, is unlikely to change much about the FTC's apparent evasion of its obligation to adhere to those standards. Rather, unless the *process* of enforcement by which the FTC has evaded the limits of the Statement is adjusted, the Commission will remain free to avoid the rigor it contemplates.

Indeed, it is far from clear that even the 1994 codification of the heart the Unfairness Policy Statement has been effective in actually changing the FTC's approach to enforcement. It is certainly possible that, but for Section 5(n), the Commission would have taken an even more aggressive approach to unfairness, and done even less to analyze its component elements in enforcement actions.

The process reforms we propose below are intended either (a) to increase the likelihood that the FTC will actually litigate unfairness cases, thus gaining judicial development of the doctrine, (b) that the Commissioners themselves will better develop doctrine through debate, or (c) that FTC staff, particularly through the involvement of the Bureau of Economics, will do so. Some combination of these (and, doubtless, other) reforms is essential to giving effect to Section 5(n) in its current form, to say nothing of expanding 5(n).

But the reform that would make the biggest difference within 5(n) itself would be to amend the existing Section 5(n) as follows:

> The Commission may not issue a complaint under this section unless the Commission demonstrates by a **preponderance of objective evidence** that an act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

The preponderance of the evidence standard is certainly a higher standard than the FTC currently faces for bringing complaints, but only because that standard is so absurdly low under Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[50] The "preponderance of the evidence" standard is the same standard used in civil cases, simply requiring that civil plaintiffs provide evidence that that their argument is "more likely than not" to get judgement against defendants. This standard is substantially less stringent than the "beyond a reasonable doubt" standard used in criminal cases, or the "clear and convincing" standard used in habeas petitions, so it should be suitable for the FTC's unfairness work.

---

[50] 15 U.S.C. § 45(b).

Why should the FTC have a higher burden (than it does today) at this intermediate stage in its enforcement process, when it brings a complaint? The FTC has significant pre-complaint powers of investigation at its disposal; it will have had considerable opportunity to perform discovery *before* bringing its complaint. Unlike private plaintiffs, who must first survive a *Twombly/Iqbal* motion to dismiss before they can compel discovery, typically at their own expense, the FTC can do so (through its civil investigative demand power) — and impose all of its costs on potential defendants — *before* ever alleging wrongdoing.

As we discuss in more detail below,[51] in order to justify the massive expense of this pre-complaint discovery process, it is not enough that it enables the Commission to engage in fishing expeditions to "uncover" possible violations of the law. Rather, if it is to be justified, and if its use by the Commission is to be kept consistent with its consumer-welfare mission, it must tend to lead to enforcement only when complaints can be justified by the weight of the evidence uncovered. A heightened burden is more likely to ensure this fealty to the consumer interest and to reduce the inefficient imposition of discovery costs on the wrong enforcement targets.

It is also important to note that, although we disagree strongly with their claims,[52] several FTC Commissioners and commentators have asserted that the set of consent orders entered into by the Commission with various enforcement targets constitute a *de facto* common law: "Technically, consent orders legally function as contracts rather than as binding precedent. Yet, in practice, the orders function much more broadly…."[53] In making these claims, proponents, including the Commission's current Chairwoman,[54] assert that "the trajectory and

---

[51] *See infra* at 31.

[52] *See, e.g.*, Berin Szóka, *Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection "Case Law,"* (2014 TPRC Conference Paper, Jul. 15, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418572; Geoffrey A. Manne & Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security*, *available at* http://masonlec.org/site/rte_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf.

[53] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 607 (2014).

[54] *Address by FTC Chairwoman Edith Ramirez,* at 6, at the Competition Law Center at George Washington University School of Law (Aug. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/735411/150813section5speech.pdf ("As I have emphasized, I favor a common law approach to the development of Section 5 doctrine."). The previous chairwoman held the same view. *See* Commissioner Julie Brill, *Privacy, Consumer Protection, and Competition*, speech given at 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-andcompetition/120427loyolasymposium.pdf ("Yet our privacy cases are also more generally informative about data collection and use practices that are acceptable, and those that cross the line, under Section 5 of the Federal Trade Commission Act creating what some have referred to as a common law of privacy in this country.").

development [of FTC enforcement] has followed a predictable set of patterns… [that amount to] the functional equivalent of common law."[55]

For these claims to be true or worthy, it would seem necessary, *at a minimum,* that the Commission's consumer protection complaints, which are virtually always coupled with consent orders upon their release (because *there is no statutory standard for settling FTC enforcement actions*), be tied to substantive standards that go beyond the mere exercise of three commissioners' discretion. And yet the FTC and the courts have consistently argued that the FTC Act's "reason to believe" standard for issuance of complaints requires nothing more than this minimal exercise of discretion. As former Commissioner Tom Rosch put it,

> [t]he "reason to believe" standard, however, is not a summary judgment standard: it is a standard that simply asks whether there is a reason to believe that litigation may lead to a finding of liability. That is a low threshold…. [T]he "reason to believe" standard is amorphous and can have an "I know it when I see it" feel."[56]

This creates a real problem for the claims that the Commission's consent orders have any kind of precedential power:

> In theory, the questions of whether to bring an enforcement action and whether a violation occurred are distinct; but in practice, when enforcement actions end in settlements (and when the two are often filed simultaneously), the two questions collapse into one. The FTC Act does not impose any additional requirement on the FTC to negotiate a settlement…. Thus, at best, the FTC's decisions are roughly analogous not to court decisions on the merits, but to court decisions on motions to dismiss…. Or, perhaps even more precisely, the FTC's decisions are analogous to reviews of warrants in criminal cases, as Commissioner Rosch has argued. It would be a strange criminal common law, indeed, that confused ultimate standards of guilt with the far lower standard of whether the police could properly open an investigation, yet this is essentially what the FTC's "common law" of settlements does.[57]

The incentives, discussed in more detail below,[58] that impel nearly every FTC consumer protection enforcement target to settle with the agency ensure that the only practical inflec-

---

[55] Solove & Hartzog, *supra* note 53, at 608.

[56] J. Thomas Rosch, Commissioner, Fed. Trade Comm'n, *Remarks at the American Bar Association Annual Meeting*, 3–4 (Aug. 5, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/so-i-serve-both-prosecutor-and-judge-whats-big-deal/100805abaspeech.pdf.

[57] Berin Szóka, *Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection "Case Law"* 7-8, available at http://masonlec.org/site/rte_uploads/files/Szoka%20for%20GMU%20FTC%20Workshop%20-%20May%202014.pdf.

[58] See *infra* at 31.

tion point at which the entire enforcement process is subject to any kind of "review," is when the Commissioners vote to authorize the issuance of a formal complaint and, simultaneously, approve an already-negotiated settlement. That such a determination may be based solely on the effectively unreviewable[59] discretion of the Commission that the complaint — not the consent order — meets the current, low threshold is troubling.

As former FTC Chairman Tim Muris observed, "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[60] If meaningful judicial review is ever to be brought to bear on the final agency decisions embodied in consent orders, it is crucial that the complaints that give rise to those settlements be subject to a more meaningful standard that imposes some evidentiary and logical burden on the Commission beyond the mere exercise of its discretion. While a preponderance of the evidence standard would hardly impose an insurmountable burden on the agency, it would at least impose a standard that is more than purely discretionary, and thus reviewable by courts and subject to recognizable standards upon which such review could proceed. Most importantly, enacting such a standard should, on the margin, embolden defendants to resist settling cases, thus producing more judicial decisions, which could in turn constrain the FTC's discretion.

None of our proposed reforms to the FTC's investigation process[61] would in any way undermine the FTC's ability to gather information prior to issuing a complaint. The FTC would still be able to contact parties and investigate them through its 6(b) powers and use civil investigative demands if necessary to compel disclosure. But it is necessary to heighten the FTC's standard for finally bringing a complaint since it can do significant investigation beforehand. It is not unreasonable to think they should have enough evidence to determine a violation of the law by a preponderance of the evidence by the point of complaint, especially since this is where most enforcement actions end in settlement.

Deception & Materiality

No Bill Proposed

The FTC's 1983 Deception Policy Statement forms one of the two pillars of its consumer protection work. As with Unfairness, the purpose of the Deception power is to protect consumers from injury. But unlike Unfairness, Deception does not require the FTC to prove injury. Instead, the FTC need prove only materiality — as an evidentiary proxy for injury:

---

[59] *See* FTC v. Standard Oil Co. of Cal., 449 U.S. 232 (1980).

[60] Muris, *supra* note 8, at 49.

[61] *See infra* at 31.

> [T]he representation, omission, or practice must be a "material" one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception. **In many instances, materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary**. Thus, the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment….[62]
>
> A finding of materiality is also a finding that injury is likely to exist because of the representation, omission, sales practice, or marketing technique. Injury to consumers can take many forms. **Injury exists if consumers would have chosen differently but for the deception**. **If different choices are likely, the claim is material, and injury is likely as well. Thus, injury and materiality are different names for the same concept**.[63]

Materiality is the *point* of the Deception Policy Statement. It is a shortcut by which the FTC can protect consumers from injury (*i.e.*, not getting the benefit of the bargain promised them) without having to establish injury (that failing to get this benefit actually harms them). A finding of materiality allows the FTC to presume injury because, in the traditional marketing context, a deceptive claim that is "material" enough to alter consumer behavior (which is the *point* of marketing, after all) may reasonably be presumed to do so in ways that a truthful claim wouldn't (or else why bother making the misleading claim?).

Unfortunately, the FTC has effectively broken the logic of the materiality "shortcut" by extending a *second* set of presumptions: most notably, that all express statements are material. This presumption may make sense in the context of traditional marketing claims, but it breaks down with things like privacy policies and other non-marketing claims (like online help pages) — situations where deceptive statements certainly *may* alter consumer behavior, but in which such an effect can't be presumed (because the company making the claim is not doing so in order to convince consumers to purchase the product).[64]

The FTC has justified this presumption-on-top-of-a-presumption by pointing to this passage of the DPS (shown with the critical footnotes):

---

[62] *DPS supra* note 10.

[63] *Id.* at 6 (emphasis added).

[64] Of course, even in the marketing context this presumption is one of administrative economy, not descriptive reality. While there is surely a correlation between statements intended to change consumer behavior and actual changes in consumer behavior, a causal assumption is not warranted. *See generally* Geoffrey A. Manne & E. Marcellus Williamson, *Hot Docs vs. Cold Economics: The Use and Misuse of Business Documents in Antitrust Enforcement and Adjudication*, 47 ARIZ. L. REV. 609 (2005).

> The Commission considers certain categories of information presumptively material.[47] First, the Commission presumes that express claims are material.[48] As the Supreme Court stated recently [in *Central Hudson Gas & Electric Co. v. PSC*], "[i]n the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising."
>
> [47] The Commission will always consider relevant and competent evidence offered to rebut presumptions of materiality.
>
> [48] Because this presumption is absent for some implied claims, the Commission will take special caution to ensure materiality exists in such cases.[65]

In effect, the first two sentences have come to swallow the rest of the paragraph, including the logic of the Supreme Court's decision in *Central Hudson,* the single most important case of all time regarding the regulation of commercial speech.[66] In particular, the FTC ignores the "absence of factors that would distort the decision to advertise."[67]

When the Deception Policy Statement talked about "express claims," it was obviously contemplating *marketing* claims, where the presumption of materiality makes sense: if a company buys an ad, anything it says in the ad is intended to convince the viewer to buy the product. The intention to advertise the product is simply the flipside of materiality — a way of inferring what reasonable buyers would think from what profit-maximizing sellers obviously intended. But this logic breaks down once we move beyond advertising claims.

We have written at length about this problem in the context of the FTC's 2015 settlement with Nomi, the maker of a technology that allowed stores to track users' movement on their premises, as well as a shopper's repeat visits, in order to deliver a better in-store shopping experience, placement of products, etc.[68]

The FTC's complaint focused on a claim made in the privacy policy on Nomi's website that consumers could opt out on the website or at "any retailer using Nomi's technology." Nomi failed to provide an in-store mechanism for allowing consumers to opt out of the tracking program, but it did provide one on the website — right where the allegedly deceptive claim was made. That Nomi did not, in fact, offer an in-store opt-out mechanism in violation of its express promise to do so is clear. Whether, taken in context, that failure was *material*, however, is not clear.

---

[65] *Id.* at 5.

[66] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of NY, 447 U.S. 557 (1980).

[67] *Id.* at 567–68.

[68] *See* Geoffrey A. Manne, R. Ben Sperry & Berin Szóka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case* (ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1), *available at* http://laweconcenter.org/images/articles/icle-nomi_white_paper.pdf.

For the FTC majority, even though the website portion of the promise was fulfilled, Nomi's failure to comply with the in-store portion amounted to an actionable deception. But the majority dodged the key question: whether the evidence that Nomi accurately promised a website opt-out, and that consumers could (and did) opt-out using the website, rebuts the presumption that the inaccurate, in-store opt-out portion of the statement was material, and sufficient to render the statement *as a whole* deceptive.

In other words, the majority assumed that Nomi's express claim, in the context of a privacy policy rather than a marketing statement, affected consumers' behavior. But given the very different purposes of a privacy policy and a marketing statement (and the immediate availability of the website opt-out in the very place that the claim was made), that presumption seems inappropriate. The majority did not discuss the reasonableness of the presumption given the different contexts, which *should* have been the primary issue. Instead it simply relied on a literal reading of the DPS, neglecting to consider whether its underlying logic merited a different approach.

The Commission failed to demonstrate that, *as a whole*, Nomi's failure to provide in-store opt out was deceptive, in clear contravention of the Deception Policy Statement's requirement that all statements be evaluated in context:

> [T]he Commission will evaluate the entire advertisement, transaction, or course of dealing in determining how reasonable consumers are likely to respond. Thus, in advertising the Commission will examine "the entire mosaic, rather than each tile separately."[69]

Moreover, despite the promise in the DPS that the Commission would "always consider relevant and competent evidence offered to rebut presumptions of materiality," the FTC failed to do so in *Nomi*. As Commissioner Wright noted in his dissent:

> [T]he Commission failed to discharge its commitment to duly consider relevant and competent evidence that squarely rebuts the presumption that Nomi's failure to implement an additional, retail-level opt out was material to consumers. In other words, the Commission neglects to take into account evidence demonstrating consumers would not "have chosen differently" but for the allegedly deceptive representation.
>
> Nomi represented that consumers could opt out on its website as well as in the store where the Listen service was being utilized. Nomi did offer a fully functional and operational global opt out from the Listen service on its website. Thus, the only remaining potential issue is whether Nomi's failure to offer the represented in-store opt out renders the statement in its privacy policy deceptive. The evi-

[69] *DPS supra* note 10, at 4 n.31 (quoting Fed. Trade Comm'n v. Sterling Drug, 317 F.2d 669, 674 (2d Cir. 1963)).

> dence strongly implies that specific representation was not material and therefore not deceptive. Nomi's "tracking" of users was widely publicized in a story that appeared on the front page of The New York Times, a publication with a daily reach of nearly 1.9 million readers. Most likely due to this publicity, Nomi's website received 3,840 unique visitors during the relevant timeframe and received 146 opt outs — an opt-out rate of 3.8% of site visitors. This opt-out rate is significantly higher than the opt-out rate for other online activities. This high rate, relative to website visitors, likely reflects the ease of a mechanism that was immediately and quickly available to consumers at the time they may have been reading the privacy policy.
>
> The Commission's reliance upon a presumption of materiality as to the additional representation of the availability of an in-store opt out is dubious in light of evidence of the opt-out rate for the webpage mechanism. Actual evidence of consumer behavior indicates that consumers that were interested in opting out of the Listen service took their first opportunity to do so. To presume the materiality of a representation in a privacy policy concerning the availability of an additional, in-store opt-out mechanism requires one to accept the proposition that the privacy-sensitive consumer would be more likely to bypass the easier and immediate route (the online opt out) in favor of waiting until she had the opportunity to opt out in a physical location. Here, we can easily dispense with shortcut presumptions meant to aid the analysis of consumer harm rather than substitute for it. The data allow us to know with an acceptable level of precision how many consumers — 3.8% of them — reached the privacy policy, read it, and made the decision to opt out when presented with that immediate choice. The Commission's complaint instead adopts an approach that places legal form over substance, is inconsistent with the available data, and defies common sense.[70]

The First Circuit's recent opinion in *Fanning v. FTC* compounds the FTC's error. First, it holds (we believe erroneously) that the DPS's presumptions aren't limited to the marketing milieu:

> There is no requirement that a misrepresentation be contained in an advertisement. The FTC Act prohibits 'deceptive acts or practices,' and we have upheld the Commission when it imposed liability based on misstatements not contained in advertisements.[71]

In addition, the *Fanning* decision would allow the FTC to go even a step further. Citing the language from the Deception Policy Statement that "claims pertaining to a central charac-

---

[70] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Nomi Technologies, Inc., at 3-4 (Apr. 23, 2015) (emphasis added), *available at* https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

[71] Fanning v. Fed. Trade Comm'n, No. 15-1520, slip op. at 13 (May 9, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/051816jerkopinion.pdf (citing *Sunshine Art Studios, Inc. v. FTC*, 481 F.2d 1171, 1173-74 (1st Cir. 1973) (finding FTC Act violation based on company's practice of sending customers excess merchandise and using "a fictitious collection agency to coerce payment")).

teristic of the product about 'which reasonable consumers would be concerned,'" are material, the First Circuit shifted the burden of proof to Fanning to prove that its promises were *not* material.

Of course, the DPS strongly suggests that this "central characteristic" language is also applicable only in the marketing context — in the context, that is, of claims made about a product's "central characteristics" in the service of *selling* that product — and that it is fact-dependent:

> Depending on the facts, information pertaining to the central characteristics of the product or service will be presumed material. Information has been found material where it concerns the purpose, safety, efficacy, or cost, of the product or service. Information is also likely to be material if it concerns durability, performance, warranties or quality.[72]

Much like *Nomi*, the effect of the First Circuit's decision could be far-reaching. If the FTC may simply assert that claims relate to the central characteristic of a product, receive a presumption of materiality on that basis, and then shift the burden the defendant to adduce evidence to the contrary, it may *never* need to offer any evidence of its own on materiality. Combined this with the reluctance of the FTC to actually consider evidence rebutting the presumption (as illustrated in *Nomi*), we could see cases where the FTC presumes materiality on the basis of mere allegation and ignores all evidence to the contrary offered in rebuttal, despite its promise to "always consider relevant and competent evidence offered to rebut presumptions of materiality.[73] This would lead to an outcome that the drafters of the Deception Policy Statement plainly did not intend: that effectively every erroneous or inaccurate word ever publicly disseminated by companies may be presumed to injure consumers and constitute an actionable violation of Section 5.

In short, if the courts will defer to the FTC even as it reads the materiality requirement out of the Deception Policy Statement, this is not a vindication of the FTC's reading; it is merely a reminder of the vastness of the deference paid to agencies in interpreting ambiguous statutes. And it should be a reminder to Congress that only through legislation can Congress ultimately reassert itself — if only to keep the FTC on the path the agency itself laid out decades ago.

RECOMMENDATION: Codify the 1983 Deception Policy Statement

Congress should codify the Deception Policy Statement in a new Section 5(o), just as it codified the core part of the Unfairness Policy Statement in 1994, and just as the SURE Act would codify the rest of the UPS today. Fully codifying both statements (all *three* statements,

---

[72] *DPS supra* note 10, at 5.

[73] *Id.* at n.47.

including the UMC Enforcement Policy Statement) is a good idea if only because the FTC is somewhat more likely to take them seriously if they are statutory mandates. But, as we have emphasized, codification alone will not do much to change the institutional structures and processes that are at the heart of the statements' relative ineffectiveness in guiding the FTC's discretion.

In codifying the DPS, Congress should be mindful of the problems we discuss above. It should also modify the DPS' operative language to mitigate the interpretative problems arising from its inevitable ambiguity. Without specifying precise language here, a few guidelines for drafting such language come readily to mind:

1. Defer to the DPS drafters: they could never have meant for the exceptions (presumptions) to subsume the rule (the materiality requirement), and the codified language should endeavor to reflect this.
2. Acknowledge that there are differences between marketing language and language used in other contexts, including, importantly, today's ubiquitous privacy policies and website terms of use — settings that weren't contemplated by the DPS drafters.
3. Clarify what evidentiary burden is required to demonstrate materiality in contexts where it shouldn't simply be inferred, and, after *Fanning*, clarify whether, and when, the burden should shift from the FTC to defendants.

RECOMMENDATION: Clarify that Legally Required Statements Cannot Be Presumptively Material

Particularly given the increasing importance of privacy policies in the FTC's deception enforcement practice, it is also important to clarify whether legally mandated language should be presumed material. We believe that the DPS' exception for "factors that would distort the decision to advertise" includes a legal mandate to say something, which unequivocally "distorts" the decision to proffer such language. Thus, in most cases, privacy policies — required by California law[74] — ought not be treated as presumptively material. This would not preclude the FTC from proving that they *are* material, of course. It would simply require the Commission to *establish* their materiality in each particular case — which, again, was the point of the Deception Policy Statement in the first place.

RECOMMENDATION: Delegate Reconsideration of Other Materiality Presumptions

Unfortunately, it will be difficult for Congress to address the other aspects of the FTC's interpretation of materiality by statute, because each is highly fact-specific. But, ultimately, ensuring that the FTC's implementation of the Deception Policy Statement's requirement of

[74] *See* CAL. BUS. & PROF. § 22575, *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579.

a rigorous assessment of trade-offs doesn't require specification of outcomes; it requires some institutional rejiggering ensure that the Bureau of Consumer Protection is motivated to do so by some combination of the courts, the commissioners, and the Bureau of Economics.

Instead of trying to address these issues directly, Congress could, for example, direct the FTC to produce a Policy Statement on Materiality in which the Commission attempts to clarify these issues on its own. Thus, for example, the Commission could describe factors for determining whether and when an online help center should be considered a form of marketing that merits the presumption. Or, as we have previously proposed, Congress could delegate this and other key doctrinal questions to a Modernization Commission focused on high-tech consumer protection issues like privacy and data security, parallel to the Antitrust Modernization Commission.[75]

RECOMMENDATION: Require Preponderance of the Evidence in Deception Cases

Above, we explain that among our top three priorities for additional reforms — indeed, for reforms overall — is adding a "preponderance of the evidence" standard for unfairness cases by expanding upon Section 5(n).[76] We urge Congress to include the same standard in a new Section 5(o) for non-fraud deception cases. Again, this standard should be easy for the FTC to satisfy.

Unfair Methods of Competition

No Bill Proposed

The Commission's unanimous adoption last year of a "Statement of Enforcement Principles Regarding 'Unfair Methods of Competition'" was a watershed moment for the agency.[77] The adoption of the Statement marked the first time in the Commission's 100-year history

---

[75] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf ("A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.").

[76] *See supra* note 18.

[77] Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

that the FTC issued enforcement guidelines for cases brought under the Unfair Methods of Competition ("UMC") provisions of Section 5 of the FTC Act.[78]

Enforcement principles for UMC actions were in desperate need of clarification at the time of the Statement's adoption. Without any UMC standards, the FTC had been essentially completely free to leverage its costly adjudication process into settlements (or short-term victories), and to leave businesses in the dark as to what sorts of conduct might trigger enforcement. Through a series of un-adjudicated settlements, UMC unfairness doctrine (such as it is) has remained largely within the province of FTC discretion and without judicial oversight. As a result, and either by design or by accident, UMC never developed a body of law encompassing well-defined goals or principles like antitrust's consumer-welfare standard. Several important cases had seemingly sought to take advantage of the absence of meaningful judicial constraints on UMC enforcement actions to bring standard antitrust cases under the provision.[79] And more than one recent Commissioner had explicitly extolled the virtue of the unfettered (and unprincipled) enforcement of antitrust cases the provision afforded the agency.[80] The new Statement makes it official FTC policy to reject this harmful dynamic.

The UMC Statement is deceptively simple in its framing:

> In deciding whether to challenge an act or practice as an unfair method of competition in violation of Section 5 on a standalone basis, the Commission adheres to the following principles:
>
> - the Commission will be guided by the public policy underlying the antitrust laws, namely, the promotion of consumer welfare;
> - the act or practice will be evaluated under a framework similar to the rule of reason, that is, an act or practice challenged by the Commission must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications; and

---

[78] It should be noted that the Statement represents a landmark victory for Commissioner Joshua Wright, who has been a tireless advocate for defining the scope of the Commission's UMC authority since before his appointment to the FTC in 2013. *See, e.g.*, Joshua D. Wright, *Abandoning Antitrust's Chicago Obsession: The Case for Evidence-Based Antitrust*, 78 ANTITRUST L. J. 241 (2012).

[79] For a succinct evaluation of these cases (including, e.g., *Intel* and *N-Data*), see Geoffrey A. Manne & Berin Szóka, *Section 5 of the FTC Act and monopolization cases: A brief primer*, TRUTH ON THE MARKET (Nov. 26, 2012), https://truthonthemarket.com/2012/11/26/section-5-of-the-ftc-act-and-monopolization-cases-a-brief-primer/.

[80] *See, e.g.*, Statement of Chairman Leibowitz and Commissioner Rosch, In the Matter of Intel Corp., Docket No. 9341, 1, *available at* https://www.ftc.gov/system/files/documents/public_statements/568601/091216intelchairstatement.pdf ("[I]t is more important than ever that the Commission actively consider whether it may be appropriate to exercise its full Congressional authority under Section 5.").

- the Commission is less likely to challenge an act or practice as an unfair method of competition on a standalone basis if enforcement of the Sherman or Clayton Act is sufficient to address the competitive harm arising from the act or practice.[81]

Most importantly, the Statement espouses a preference for enforcement under the antitrust laws over UMC when both might apply, and brings the weight of consumer-welfare-oriented antitrust law and economics to bear on such cases.

RECOMMENDATION: Codify the Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under a New Section 5(p) of the FTC Act

As beneficial as the Statement is, it necessarily reflects compromise. In particular, the third prong is expressed merely as a *preference* for antitrust enforcement rather than an obligation. And, of course, such statements are not binding on the Commission, no matter how strongly worded they may be, and no matter how much "soft law" may be brought to bear on the Commissioners charged with following it.

For these reasons, Congress should codify the most important aspects of the Statement — much as it did with the Unfairness Policy Statement's consumer-injury unfairness test — by adding the following language in a new Section 5(p):

> The Commission ***shall not*** challenge an act or practice as an unfair method of competition on a standalone basis if the alleged competitive harm arising from the act or practice is subject to enforcement under the Sherman or Clayton Act.
>
> An act or practice challenged by the Commission as an unfair method of competition must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications.

This language is taken directly from the UMC Statement, with the small tweak highlighted above *requiring* application of the antitrust laws instead of UMC in appropriate cases, rather than merely expressing a preference for doing so.

Such language would harmonize enforcement of all anticompetitive practices under the antitrust laws' consumer-welfare standard, while still permitting the few cases not amenable to Sherman or Clayton Act jurisdiction (*e.g.*, invitations to collude) to be brought by the Commission. Importantly, language such as this, which would make enforcement under the antitrust laws *obligatory* where both UMC and antitrust could apply, would transform the Statement's expression of agency preference into an enforceable statutory requirement.

---

[81] Statement of UMC Enforcement Principles, *supra* note 77.

Enforcement & Guidance

The FTC is commonly labeled a "law enforcement agency," but in reality it is an administrative agency that regulates primarily through enforcement rather than rulemaking:

> As an administrative agency, the FTC's primary form of regulation involves administrative application of a set of general principles — a "law enforcement" style function that, practically speaking, operates as administrative regulation….[82]

This administrative enforcement model puts significant emphasis on the agency's investigative power, and it is the investigatory aspect of its enforcement process that has become the agency's most powerful — and least overseen — tool. As one commentator notes, "[t]he FTC possesses what are probably the broadest investigatory powers of any federal regulatory agency."[83]

The Commission's investigatory process is also the heart of the mechanism by which the agency largely bypasses judicial oversight:

> [Not even] the courts have… been a significant factor in deterring FTC investigation. Indeed, the bulk of court cases appear to affirm the agency's authority to obtain information pursuant to the Federal Trade Commission Act. Thus, any constraints placed upon the FTC's ability to obtain information must lie elsewhere.[84]

By overly compelling companies to settle enforcement actions when they are little more than investigations, the investigative process inevitably leads, on the margin, to less-well-targeted investigations, increased discovery burdens on (even blameless) potential defendants, inefficiently large compliance expenditures throughout the economy, under-experimentation and innovation by firms, doctrinally questionable consent orders, and a relative scarcity of judicial review of Commission enforcement decisions.

More than any other aspect of the FTC Act or the FTC's operations, it is here that reinvigorated congressional oversight is needed. Even Chris Hoofnagle, who has long advocated that the FTC be far more aggressive on privacy and data security, warns, in his new treatise on privacy regulation at the agency, that

---

[82] *Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission*, *supra* note 4, at 12.

[83] Stephanie W. Kanwit, 1 Federal Trade Commission § 13:1 at 13-1 (West 2003).

[84] Darren Bush, *The Incentive and Ability of the Federal Trade Commission to Investigate Real Estate Markets: An Exercise in Political Economy*, 20-21, *available at* http://www.antitrustinstitute.org/files/517c.pdf.

> the FTC's investigatory power is very broad and is akin to an inquisitorial body. On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[85]

In competition cases, the entire Commission must vote to authorize CIDs in each matter and also vote to close investigations once compulsory process is issued. But in the consumer protection context, the Commission issues standing orders — "omnibus resolutions" (ORs) — authorizing extremely broad, industry-wide investigations that authorize the subsequent issuance of CIDs with the consent of only a single Commissioner. For instance, there is a standing Commission order authorizing staff to investigate telemarketing fraud cases.[86] Thus, if staff wants to issue a CID to investigate a specific telemarketer or any of a wide range of companies that may be supporting telemarketers, it need seek approval for the CID from only a single Commissioner. These requests are frequent (to the best of our knowledge amounting to many dozens *per week*), and routinely granted.

The staff's ability to rely upon Omnibus Resolutions in this manner bypasses an important aspect of how the FTC's enforcement approach is structured on paper. The FTC Operating Manual draws a clear line between initial phase investigations (initiated and run by the staff at their own discretion for up to 100 hours in consumer protection cases) and full investigations. The decision to upgrade an investigation can be made by the Bureau Director on delegated authority, but at least this creates some potential for involvement of other Commissioners. It also requires written analysis by the staff[87] — something other Commissioners could ask to see. But most relevant to the immediate discussion is the Commission's policy that

> Compulsory procedures are not ordinarily utilized in the initial phase of investigations; therefore, facts and data which cannot be obtained from existing sources must be developed through the use of voluntary procedures.[88]

Relying on ORs, however, the staff may make use of compulsory process even when it would not otherwise be appropriate to do so.

At the same time, the Commission may (if it so chooses) bring its Section 5 cases (those relatively few that don't settle) in its own administrative tribunal, whose decisions are appealed to the Commission itself. Only after the Commission's review (or denial of review) may a

---

[85] HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY, *supra* note 3, at 102.

[86] Resolution No. 0123145, "Resolution Directing the Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, and Others" Technically the Telemarketing Resolution expired in April 2016. But it authorizes continuing investigation subject to already-issued CIDs as long as necessary. Although no further CIDs will be issued, the investigation continues.

[87] Federal Trade Commission, *Operating Manual*, 3.5.1.2 [hereinafter Operating Manual].

[88] *Id.* at 3.2.3.2.

party bring its case before an Article III court. Needless to say, this adds an extremely costly layer of administrative process to enforcement, as former Commissioner Wright explains:

> [T]he key to understanding the threat of Section 5 is the interaction between its lack of boundaries and the FTC's administrative process advantages.... Consider the following empirical observation that demonstrates at the very least that the institutional framework that has evolved around the application of Section 5 cases in administrative adjudication is quite different than that faced by Article III judges in federal court in the United States. The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, **in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed**. By way of contrast, when the antitrust decisions of federal district court judges are appealed to the federal courts of appeal, plaintiffs do not come anywhere close to a 100 percent success rate. Indeed, the win rate is much closer to 50 percent.[89]

The net effect of these procedural circumstances is stark. Wright continues:

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may not [violate any law or regulation]. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's [Section 5] authority by **encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority**.[90]

Further, the Commission currently enjoys a nearly insurmountable presumption that its omnibus resolutions are proper — a fact that places subjects of investigations at a severe disadvantage when trying to challenge the Commission's often intrusive investigative process.

Whether issued under an Omnibus Resolution or otherwise, the Commission's CIDs allow the agency to impose enormous costs on potential defendants before even a single Commis-

---

[89] Joshua Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, CPI ANTITRUST CHRONICLE (Nov. 2013 (2)), at 4 (emphasis added), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf.

[90] *Id.* at 5 (emphasis added).

sioner — let alone the entire Commission or a court of law — determines that there is even a "reason to believe" that the party being investigated has violated any law.

The direct costs of compliance with these extremely broad CIDs can be enormous. Unlike discovery requests in private litigation, reimbursement of costs associated with CID compliance is not available, even if a defendant prevails. Among other things, CID recipients will be required to incur the expense of performing electronic and offline searches for copious amounts of information (which may require the hiring of outside vendors), interviewing employees, the business costs of lost employee and management time, and attorneys' fees. Moreover, there may be several CIDs issued to a single company. And, sometimes of greatest importance, in many cases publicly traded companies will be required to disclose receipt of a CID in its SEC filings. This can have significant immediate effects on a company's share price and do lasting damage to its reputation among consumers.

The experience of Wyndham Hotels is illustrative. The company became the first to challenge an FTC data security enforcement action following more than twelve years of FTC data security settlements. Even before it finally had recourse to an Article III court, Wyndham had already incurred enormous costs, as we noted in our amicus brief in support of Wyndham's 2013 motion to dismiss:

> Burdensome as settlements can be, *not* settling can be even costlier. Wyndham, for example, has already received 47 document requests in this case and spent $5 million responding to these requests. The FTC's compulsory investigative discovery process and administrative litigation both consume the most valuable resource of any firm: the time and attention of management and key personnel.[91]

And it is difficult for CID recipients to challenge a CID on the basis of cost. As the Commission notes in a ruling denying one such request:

> WAM [West Asset Management] has not satisfied its burden of demonstrating compliance with the CID would be unduly burdensome…. WAM has not cited, and the Commission is unaware of, any cases to support WAM's minimize-disruption standard. "Thus courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business." As in *Texaco* the breadth of the CID is a reflection of the comprehensiveness of the inquiry being undertaken and the magnitude of WAM's business operations.[92]

---

[91] Amici Curiae Brief Of TechFreedom, International Center for Law and Economics & Consumer Protection Scholars, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 2:13-cv-01887 (3d Cir. 2013) at 13.

[92] Request for Review of Denial of Petition to Limit Civil Investigative Demand, File No. 0723006 (Jul. 2, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/west-asset-management-inc./080702westasset.pdf (citing Fed. Trade Comm'n v. Texaco, Inc., 555 F.2d 862, 882 (D.C. Cir. 1977)).

High costs, as long as they don't threaten a company's viability, will be insufficient to quash or even minimize the scope of a CID. But even expenses that don't threaten viability can be extremely large and extremely burdensome. And, of course, broader costs (*e.g.*, on stock price and market reputation) are extremely difficult to measure and unaccounted for in the FTC's assessment of a CID's burden.

It should be noted that, unlike complaints (before adjudication) and consent orders, CIDs are directly reviewed by courts at times. For better or worse, however, courts are prone to give the Commission an extreme degree of deference when reviewing CIDs. "The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one… The requested material, therefore, need only be relevant to the investigation — the boundary of which may be defined quite generally."[93] Thus, the Commission has "'extreme breadth' in conducting … investigations."[94]

But high *direct* costs aren't even the most troubling part. The indirect, societal cost of overly broad CIDs is the increased propensity of companies to settle to avoid them. For reasons we also discuss elsewhere, an excessive tendency toward settlements imposes costs throughout the economy. Among other things:

- It reduces the salutary influence of judicial review of agency enforcement actions;
- It reduces the stock of judicial decisions from which companies, courts and the FTC would otherwise receive essential guidance regarding appropriate enforcement theories and the propriety of ambiguous conduct;
- It induces companies that haven't violated the statute to be saddled with remedies nonetheless, and thereby induces other, similarly-situated companies to incur inefficient costs to avoid the same fate;
- It incentivizes the FTC to impose remedies via consent order that a court might not sustain; and
- It may induce companies that would be found by a court not to have violated the statute to admit liability.

These largely hidden, underappreciated effects are, collectively, enormously distorting. And they feedback into the process, reinforcing the institutional dynamics that lead to such outcomes in the first place. In short, the FTC's discovery process greatly magnifies its already vast discretion to make substantive decisions about the evolution of Section 5 doctrine (or quasi-doctrine).

---

[93] Invention Submission, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing Fed. Trade Comm'n v. Carter, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

[94] *Re: LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand; and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand (*Apr. 20, 2012), 5, *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./102-3099-lab-md-letter-ruling-04202012.pdf.

At the same time, there is reason to believe that the rate of CID issuance, and the scope of CIDs issued, are (far) greater than optimal.

In order to issue a CID pursuant to an OR, staff need not present the authorizing Commissioner with a theory of the case or anything approaching "probable cause" for the CID; rather, the OR effectively takes care of that (although without anything like the specificity required of, say, a subpoena), and staff need only assert that the CID is in furtherance of an OR. The other Commissioners do not have an opportunity to vote on the issuance of the CID and would not likely even know about the investigation. Even if dissenting staff members attempt to notify Commissioners,[95] it may be difficult, at this early stage, for Commissioners to recognize the doctrinal or practical significance of the cases the staff is attempting to bring, and thus to provide any meaningful check upon the discretion of the staff to use the discovery process to coerce settlements.

Thus, because of omnibus resolutions, a great number of investigations — encompassing a great number of costly CIDs — are not presented to the other Commissioners to determine whether the investigation is an appropriate use of the agency's resources or whether the legal basis for the case is sound. In many cases, the other Commissioners may not even see the case until a settlement has been negotiated as a *fait accompli*.

The bar for issuing CIDs pursuant to an omnibus resolution is extremely low. Nominally the CID request must fall within the agency's authority and be relevant to the investigation that authorizes it. But the FTC has enormous discretion in determining whether a specific compulsory demand is relevant to an investigation, and it need not have "a justifiable belief that wrongdoing has actually occurred."[96]

For example, the Commission's telemarketing resolution authorized compulsory process

> [t]o determine whether unnamed telemarketers, sellers, or others assisting them have engaged in or are engaging in: (1) unfair or deceptive acts or practices in or affecting commerce in violation of Section 5 of the Federal Trade Commission Act; and/or (2) deceptive or abusive telemarketing acts or practices in violation of the Commission's Telemarketing Sales Rule, including but not limited to the provision of substantial assistance or support — such as mailing lists, scripts, merchant accounts, and other information, products, or services — to telemarketers engaged in unlawful practices. The investigation is also to determine

[95] Operating Manual § 3.5.1.1 ("Dissenting staff recommendations regarding compulsory process, compliance, consent agreements, proposed trade regulation rules or proposed industrywide investigations should be submitted to the Commission by the originating offices, upon the request of the staff member.").

[96] United States v. Morton Salt Co., 338 U.S. 632, 642 (1950).

> whether Commission action to obtain redress for injury to consumers or others would be in the public interest.[97]

Pursuant to this OR, the Commission issued a CID to Western Union. Western Union challenged the CID on the grounds that it was unrelated to the OR (among other things). The FTC, in denying the motion to quash, claimed that "[t]he resolution… includes investigations of telemarketers or sellers as well as entities such as Western Union who may be providing substantial assistance or support to telemarketers or sellers." While the OR does mention "assistance or support," it doesn't specify any companies by name and doesn't specify that payment processors provide the sort of support it contemplates. In fact, it is fairly clear from even the impressively broad characterization of these in the OR — "mailing lists, scripts, merchant accounts, and other information, products, or services" — that the ancillary processing of payment transactions by legitimate companies was not really contemplated.

Nevertheless, the standard of review for the relevance of CIDs — in the rare instance that they are challenged at all — is extremely generous to the agency. As the Commission notes in its *Western Union* decision:

> In the context of an administrative CID, "relevance" is defined broadly and with deference to an administrative agency's determination. An administrative agency is to be accorded "extreme breadth" in conducting an investigation. As the D.C. Circuit has stated, the standard for judging relevance in an administrative investigation is "more relaxed" than in an adjudicatory proceeding. As a result, the agency is entitled to the documents unless the CID recipient can show that the agency's determination is "obviously wrong" or the documents are "plainly irrelevant" to the investigation's purpose. We find that Western Union has not met this burden.[98]

Finally, administrative challenges to CIDs are public proceedings, which itself presents a substantial bar to their review. Companies subject to investigations by the FTC are, not surprisingly, reluctant to reveal the existence of such an investigation publicly. While the immense breadth and vagueness of the ORs authorizing compulsory process in an investigation, the ease with which CIDs are issued, and the lack of a "belief of wrongdoing" requirement certainly mean that no wrongdoing *should* be inferred from the existence of an investigation or a CID, unfortunately public perception may not track these nuances. In the

---

[97] *Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others*, File No. 0123145 (Apr. 11, 2011), quoted in *In the Matter of December 12, 2012 Civil Investigative Demand Issue to the Western Union Company*, File No. 012 3145 (Mar. 4, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/unnamed-telemarketers-others/130404westernunionpetition.pdf (Citations omitted).

[98] *In the Matter of December 12, 2012 Civil Investigative Demand Issue to the Western Union Company* at 8. (Citing cases).

case of some publicly traded companies, the mere issuance of a CID may require disclosure.[99] But for other publicly traded companies and for all private companies such disclosure is not required. This means that, for these companies, there is an added deterrent to challenging a CID because doing so will cause it to be disclosed publicly when it otherwise would not be.

The combination of an exceedingly deferential standard of review, the need to exhaust administrative process before the very agency that issued the OR and CID *before* gaining access to an independent Article III tribunal, the risk of reputational harms, and the massive compliance costs combine to ensure that very few CIDs are ever challenged. This only reinforces FTC staff's incentives to issue CIDs, and to do so with an increasingly tenuous relationship to the Commission-approved resolution authorizing them.

The absence of effective oversight on this process creates a further problem. FTC staff have the power to issue Voluntary Access Letters requesting the same documents as a CID without *any* Commissioner involvement — or even (at least on paper) the possibility that a dissenting staff member can notify a Commissioner of her objections.[100] While these requests are nominally voluntary, the omnipresent threat of compelled discovery means that recipients virtually always comply with these requests, although they do often initiate a discussion between staff and recipients that may result in a narrowing of the requests' scope. Voluntary Access Letters are subject to even less scrutiny than CIDs, and there is virtually no way for any of the FTC's oversight bodies (Congress, the courts, the public, the executive branch, etc.) to monitor their use.

Investigations and Reporting on Investigations

The Clarifying Legality & Enforcement Action Reasoning (CLEAR) Act

While identifying the problems with the Commission's investigation and CID process is fairly straightforward, identifying solutions is not so straightforward. A critical first step, however, would be imposing greater transparency requirements on the Commission's investigation practices.

---

[99] *See, e.g.*, Deborah S. Birnbach, *Do You Have to Disclose a Government Investigation?*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION (May 21, 2016), https://corpgov.law.harvard.edu/2016/04/09/do-you-have-to-disclose-a-government-investigation/.

[100] Again, Operating Manual Section 3.3.5.1.1 requires that "[d]issenting staff recommendations… be submitted to the Commission by the originating offices, upon the request of the staff member," but does not include voluntary assistance letters in the list of covered subjects, only "compulsory process."

Rep. Brett Guthrie's (R-KY) proposed CLEAR Act (H.R. 5109)[101] would require the FTC to report annually to Congress on the status of its investigations, including the legal analysis supporting the FTC's decision to close some investigations without action. This requirement would not require the Commission to identify its targets, thus preserving the anonymity of the firms in question.

VALUE OF THE BILL: Better Reporting of FTC Enforcement Trends

The FTC used to provide somewhat clearer data on the number of enforcement actions it took every year, classifying each by product and "type of matter."[102] The FTC's recent "Annual Highlights" reports do not include even this level of data on its enforcement actions. [103] But neither includes the basic data required by the CLEAR Act on the number of investigations commenced, closed, settled or litigated. Without hard data on this, it is difficult to assess how the FTC's enforcement approach works, the relationship between the agency's investigations and enforcement actions, and how these has changed over time. While the bill does not specifically mention consent decrees among the items that must be reported to Congress, it does require that the report include "the disposition of such investigations, if such investigations have concluded and resulted in official agency action," which would include consent decrees.

RECOMMENDATION: Add Discovery Tools to the Required Reporting

The bill omits, however, one of the most important aspects of the FTC's operations, which is very easily quantifiable: the FTC's use of its various discovery tools. The FTC should, in addition, have to produce aggregate statistics on its use of discovery tools, excluding the specific identity of the target, but including, for example:

- The source of the investigation (*e.g.*, Omnibus Resolution, consumer complaint, etc.);
- The volume of discovery requested;
- The volume of discovery produced;
- The time elapsed between the initiation of the investigation and the request(s);
- The time elapsed between the request(s) and production;
- Estimated cost of compliance (as volunteered by the target);

---

[101] The Clarifying Legality and Enforcement Action Reasoning Act, H.R. 5109, 114th Cong. (2016) [hereinafter CLEAR Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5109/text.

[102] *See. e.g.,* 1995 Annual Report at 49, https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-1995/ar1995_0.pdf.

[103] Fed. Trade Comm'n, FTC Annual Reports, https://www.ftc.gov/policy/reports/policy-reports/ftc-annual-reports.

- The specific tool(s) used to authorize the investigation and production request(s) (*e.g.*, Omnibus Resolution, CID, Voluntary Access Letter, etc.);
- Who approved the investigation and production request(s) (*e.g.*, a single Commissioner, the full Commission, the Bureau Director, the staff itself, etc.);
- The approximate size (number of employees) and annual revenues of the target business (to measure effects on small businesses); and
- The general nature of the issue(s) connected to the investigation and production request(s).

This reporting could be largely automated from the FTC database used to log investigations, discovery requests and resulting production of documents. And, of course, the FTC should have such a flexible and usable database if it does not already. Once created, it should be relatively easy to make the data public, as it will require little more than obscuring the identity of the target, putting the size of the company in ranges, and ensuring that the metadata identifying the relevant issues is sufficiently high level (e.g., "data security" rather than "PED skimming").

VALUE OF THE BILL: What is *Not* Prohibited Is a Crucial Form of Guidance

Clarity as to what the law does *not* prohibit may be a more important hallmark of the Evolutionary Model (the *true* common law), than is specificity as to what the law does prohibit.

The FTC used to issue closing letters regularly but stopped providing meaningful guidance at least since the start of this Administration. The FTC Operating Manual already requires staff to produce a memo justifying closure of any investigation that has gone beyond the initial stage, thus requiring the approval of the Bureau Directors to expand into a full investigation, that "summarize[s] the results of the investigation, discuss[es] the methodology used in the investigation, and explain[s] the rationale for the closing."[104]

In other words, the staff already, in theory, does the analysis that would be required by the bill (at least for cases that merit being continued beyond the 100 hours allowed for initial phase consumer protection investigations);[105] they simply do not share it. Thus, at most, the bill would require (i) greater rigor in the memoranda that staff already writes, (ii) that some version of memoranda be included in the annual report, edited to obscure the company's identity, and (iii) that *some* analysis be written for initial phase cases that may be closed without any internal memoranda. And this last requirement should not be difficult for the staff to satisfy, since cases that did not merit full investigations ought to raise simpler legal issues.

---

[104] Operating Manual § 3.2.4.1.1 (consumer protection) & § 3.2.4.1.2 (competition)

[105] Operating Manual § 3.2.2.1.

For example, in 2007, the FTC issued a no-action letter closing its investigation into Dollar Tree Stores that offers a fair amount of background on the issue: "PED skimming," the tampering with of payment card PIN entry devices (PEDs) used at checkout that allowed hackers to steal customers' card information and thus make fraudulent purchases.[106] The FTC explained its decision to close the Dollar Tree Stores investigation at length, listing the factors considered by the FTC:

> the extent to which the risk at issue was reasonable foreseeable at the time of the compromise; the nature and magnitude of the risk relative to other risks; the benefits relative to the costs of protecting against the risk; Dollar Tree's overall data security practices, the duration and scope of the compromise; the level of consumer injury; and Dollar Tree's prompt response to the incident.[107]

The letter went on to note:

> We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. The staff notes that, in recent months, the risk of PED skimming at retain locations has been increasingly identified by security experts and discussed in a variety of public and business contexts. We also understand that some businesses have now taken steps to improve physical security to deter PED skimming, such as locking or otherwise securing PERs in checkout lanes; installing security cameras or other monitoring devices; performing regular PED inspections to detect tampering, theft, or other misuse; and/or replacing older PEDs with newer tamper-resistant and tamper-evident models. We hope and expect that all businesses using PEDs in their stores will consider implementing these and/or other reasonable and appropriate safeguards to secure their systems.[108]

The FTC has issued only one closing letter in standard data security cases since its 2007 letter in *Dollar Tree Stores* — and, apparently, about the same issue. In 2011, the FTC issued a letter closing its investigation of the Michaels art supply store chain.[109] The letter offers essentially no information about the investigation or analysis of the issues involved — in marked contrast to the *Dollar Tree Stores* letter. But based on press reports from 2011, the issue appears to have been the same as in *Dollar Tree Stores*: "crooks [had] tampered with PIN

---

[106] Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (June 5, 2001) *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf.

[107] *Id.* at 2.

[108] *Id.*

[109] Letter from Maneesha Mithal, Associate Director of Fed. Trade Comm'n to Lisa J. Sotto, Counsel to Michael's Stores, Inc. (June 5, 2001) *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-stores-inc./120706michaelsstorescltr.pdf.

pads in the Michaels checkout lanes, allowing them to capture customers' debit card and PIN numbers."[110]

Once again, the FTC has become increasingly unwilling to constrain its own discretion, even in the issuance of closing letters that do not bar the FTC from taking future enforcement actions. This underscores not only the value of the CLEAR Act, but also of the challenge in getting the FTC to take seriously the bill's requirement that annual reports include, "for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation."[111]

RECOMMENDATION: Require the Bureau of Economics to Be Involved

Wherever possible, Congress should specify that the Bureau of Economics be involved in the making of important decisions, and in the production of important guidance materials. Absent that instruction, the FTC, especially the Bureau of Consumer Protection, will likely resist fully involving the Bureau of Economics in its processes. The simplest way to make this change is as follows:

> For each such investigation that was closed with no official agency action, a description sufficient to indicate the legal ***and economic*** analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

Of course, there will be many cases where the economists have essentially nothing to say. The point is not that each case merits detailed economic analysis. Rather, the recommendation is intended to ensure that, at the very least, the *opportunity* to produce and disseminate a basic economic analysis by the BE is built into the enforcement process.

Moreover, if an economic analysis is deemed appropriate, the determination of what constitutes an appropriate *level* of analysis should be made by the Bureau of Economics alone. For example, in the *Dollar Tree Stores* letter quoted above, it would have been helpful if the letter had provided *some* quantitative analysis as to the factors mentioned in the letter. To illustrate this point, one might ask the following questions about the factors identified in *Dollar Tree Stores*:

- "the extent to which the risk at issue was reasonably foreseeable at the time of the compromise" and "the nature and magnitude of the risk relative to other

---

[110] Elisabeth Leamy, *Debit Card Fraud Investigation Involving Michaels Craft Stores PIN Pads Spreads to 20 US States*, ABC NEWS (May 13, 2011) *available at* http://abcnews.go.com/Business/ConsumerNews/debit-card-fraud-michaels-crafts-customers-info-captured/story?id=13593607.

[111] CLEAR Act, *supra* note 101.

risks" — ***How widely known was the vulnerability generally at that time? How fast was awareness spreading among similarly situated companies? How likely was the vulnerability to occur?***

- "the benefits relative to the costs of protecting against the risk" — ***Given the impossibility of completely eradicating risk, how much ex ante "protection" would have been sufficient? Given the* ex ante *uncertainty of any particular risk occurring, how much would it have cost to mitigate against all such risks, not just the one that actually materialized?***
- "Dollar Tree's overall data security practices" — ***How much did the company spend? How else do its practices compare to its peers? How can good data security be quantified?***
- "the duration and scope of the compromise" — ***How long? How many users?***
- "the level of consumer injury" — ***Can this be quantified specifically to this case? Or can injury be extrapolated from reliably representative samples of similar injury?***
- "Dollar Tree's prompt response to the incident" — ***Just how prompt was it, in absolute terms? And relative to comparable industry practice?***

Given the general scope of the FTC's investigations, it likely already collects the kind of data that could allow it to answer some, if not all, of these questions (and others as well). It may even have performed some of the requisite analysis. Why should the Commission's economists not have a seat at the table in writing the closing analysis? This could be perhaps the greatest opportunity to begin bringing the analytical rigor of law and economics to consumer protection.

Of course, the Commission may be (quite understandably) reluctant to include this data in company-specific closing letters — for the same reasons that investigations are supposed to remain confidential. But therein lies one of the chief virtues of the CLEAR Act: Instead of writing company-specific letters, the FTC could aggregate the information, obscure the identity of the company at issue in each specific case, and thus speak more freely about the details of its situation. Although the tension between the goals of providing analytical clarity and maintaining confidentiality for the subjects of investigation is obvious, it is not an insurmountable conflict, and thus no reason not to require more analysis and disclosure, in principle.

Finally, it is worth noting that if BE is to be competent in its participation in these investigations and the associated reports, it will need a larger staff of economists. Thus, as we discuss below, Congress should devote additional resources to the Commission that are specifically earmarked for hiring additional BE staff.[112]

[112] *See infra* note 123.

RECOMMENDATION: Attempt to Make the FTC Take the Analysis Requirement Seriously

We recommend that Congress emphasize *why* such reporting is important with something like the following language, added either to Congressional findings or made clear in the legislative history around the bill:

- Guidance from the Commission as to what is *not* illegal may be the most important form of guidance the Commission can offer; and
- To be truly useful, such guidance should hew closely the FTC's applicable Policy Statements.

We further recommend that Congress carefully scrutinize the FTC's annual reports issued under the CLEAR Act in oral discussions at hearings and in written questions for the record. Indeed, *not* doing so will indicate to the FTC that Congress is not really serious about demanding greater analytical rigor.

RECOMMENDATION: Ensure that the Commission Organizes These Reports in a Useful Manner

The legal analysis section of the bill is markedly different from the other three sections. The first two sections require simple counts of investigations commenced and closed with no action. The third section ("disposition of such investigations, if such investigations have concluded and resulted in official agency action") can be satisfied with a brief sentence for each (or less). But the fourth section requires long-form analysis, which could run many pages for each case.

At a minimum, the FTC should do more than it does today to make it easy to identify which closing letters are relevant. Today, the Commission's web interface for closing letters is essentially useless. Letters are listed in reverse chronological order with no information provided other than the name, title and corporate affiliation of the person to whom the letter is addressed. There is no metadata to indicate what the letter is about (e.g., privacy, data security, advertising, product design) or what doctrinal issues (*e.g.,* unfairness, deception, material omissions, substantiation) the letter confronts. Key word searches for, say, "privacy" or "data security" produce zero results.

The CLEAR Act offers Congress a chance to demand better of the Commission. Congress should communicate what a *useful* discussion of closing decisions might look like — whether by including specific instructions in legislation, by addressing the issue in legislative history, or simply (and probably least effectively in the long term) by raising the issue regularly with the FTC at hearings. For instance, the text in the FTC's reports to Congress could be made publicly available in an online database tagged with metadata to make it easier for users to search for and find relevant closing letters.

Ideally, this database would be accessed through the same interface envisioned above for transparency into the FTC's discovery process, and would include the same metadata and

search tools. Thus, a user might be able to search for FTC enforcement actions and discovery inquiries regarding, say, data security practices in small businesses, in order to get a better sense of how the FTC operates in that area.

RECOMMENDATION: Require the FTC to Synthesize Closing Decisions and Enforcement Decisions into Doctrinal Guidelines

When the FTC submitted the Unfairness Policy Statement to Congress, it noted, in its cover letter:

> In response to your inquiry we have therefore undertaken a review of the decided cases and rules and have synthesized from them the most important principles of general applicability. Rather than merely reciting the law, we have attempted to provide the Committee with a concrete indication of the manner in which the Commission has enforced, and will continue to enforce, its unfairness mandate. In so doing we intend to address the concerns that have been raised about the meaning of consumer unfairness, and thereby attempt to provide a greater sense of certainty about what the Commission would regard as an unfair act or practice under Section 5.[113]

This synthesis is what the FTC needs to do now — and could get close to doing, in part, through better organized reporting on its closing decisions — only on a more specific level of the component elements of each of its Policy Statements. This is essentially what the various Antitrust Guidelines issued jointly by the DOJ and the FTC's Bureau of Competition do. These are masterpieces of thematic organization. Consider, for example, from the 2000 Antitrust Guidelines for Collaborations Among Competitors, this sample of the table of contents:

> **3.34** Factors Relevant to the Ability and Incentive of the Participants and the Collaboration to Compete
> - **3.34(a)** Exclusivity
> - **3.34(b)** Control over Assets
> - **3.34(c)** Financial Interests in the Collaboration or in Other Participants
> - **3.34(d)** Control of the Collaboration's Competitively Significant Decision Making
> - **3.34(e)** Likelihood of Anticompetitive Information Sharing
> - **3.34(f)** Duration of the Collaboration

> **3.35** Entry

> **3.36** Identifying Procompetitive Benefits of the Collaboration
> - **3.36(a)** Cognizable Efficiencies Must Be Verifiable and Potentially Procompetitive

[113] UPS, *supra* note 9.

3.36(b) Reasonable Necessity and Less Restrictive Alternatives
3.37 Overall Competitive Effect[114]

The guidelines are rich with examples that illustrate the way the agencies will apply their doctrine. As noted in the introduction, these guidelines are one level down the Doctrinal Pyramid: They explain how the kind of concepts articulated at the high conceptual level of, say, the FTC's UDAP policy statements, can actually be applied to real world circumstances.[115]

One obvious challenge is that the antitrust guidelines synthesize litigated cases, of which the FTC has precious few on UDAP matters. This makes it difficult, if not impossible, for the FTC to do *precisely* the same thing on UDAP matters as the antitrust guidelines do. But that does not mean the FTC could not benefit from writing "lessons learned" retrospectives on its past enforcement efforts and closing letters.

Importantly, publication of these guidelines would not actually be a constraint upon the FTC's discretion; it would merely require the Commission to better explain the rationale for what it has done in the past, connecting that arc across time. Like policy statements and consent decrees, guidelines are not technically binding upon the agency. Yet, in practice, they would steer the Commission in a far more rigorous way than its vague "common law of consent decrees [or of congressional testimony or blog posts]." It would allow the FTC to build doctrine in an analytically rigorous way as a second-best alternative to judicial decision-making — and, of course, as a supplement to judicial decisions, to the extent they happen.

RECOMMENDATION: Ensure that Defendants Can Quash Subpoenas Confidentially

Among the biggest deterrents to litigation today is companies' reluctance to make public investigations aimed at them. But a company wishing to challenge the FTC's overly broad investigative demands effectively must accede to public disclosure because the FTC has the discretion to make such fights public.

Specifically, FTC enforcement rules currently allow parties seeking to quash a subpoena to ask for confidential treatment for their motions to quash, but the rules also appear to set public disclosure as the default:

---

[114] FED. TRADE COMM'N & DEP'T OF JUSTICE, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS ii (Apr. 2000), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

[115] *See supra* note 12.

> (d) **Public disclosure**. All petitions to limit or quash Commission compulsory process and all Commission orders in response to those petitions shall become part of the public records of the Commission, except for information granted confidential treatment under § 4.9(c) of this chapter.[116]

The referenced general rule on confidentiality gives the FTC's General Counsel broad discretion in matters of confidentiality:

> (c) **Confidentiality and in camera material**.
>
> (1) Persons submitting material to the Commission described in this section may designate that material or portions of it confidential and request that it be withheld from the public record. All requests for confidential treatment shall be supported by a showing of justification in light of applicable statutes, rules, orders of the Commission or its administrative law judges, orders of the courts, or other relevant authority. **The General Counsel or the General Counsel's designee will act upon such request with due regard for legal constraints and the public interest**.[117]

Setting the default to public disclosure for such disputes is flatly inconsistent with the FTC's general policy of keeping investigations nonpublic:

> While investigations are generally nonpublic, Commission staff may disclose the existence of an investigation to potential witnesses or other third parties to the extent necessary to advance the investigation.[118]

This is the right balance: Commission staff should *sometimes* be able to disclose aspects of an investigation. It should *not* be able to coerce a company into settling, or complying with additional discovery, in order to avoid bad press. Even if a company calculates that bad press is inevitable, if the FTC seems determined to extract a settlement, disclosing the investigation earlier can increase the direct expenses and reputational costs incurred by the company by stretching out the total length of the fight with the Commission for months or years longer.

---

[116] 16 C.F.R. § 2.10(d).

[117] 16 C.F.R. § 4.9(c)(1).

[118] 16 C.F.R. § 2.6; *See also* Federal Trade Commission, *Operating Manual*, Section 3.3.1 (To promote orderly investigative procedures and to protect individuals or business entities under investigation from premature adverse publicity, the Commission treats the fact that a particular proposed respondent is under investigation and the documents and information submitted to or developed by staff in connection with the investigation as confidential information that can be released only in the manner and to the extent authorized by law and by the Commission. In general, even if a proposed respondent in a nonpublic investigation makes a public disclosure that an investigation is being conducted, Commission personnel may not acknowledge the existence of the investigation, or discuss its purpose and scope or the nature of the suspected violation.)

We propose that the default be switched, so that motions to quash are generally kept under seal except in exceptional circumstances.

Economic Analysis of Investigations, Complaints, and Consent Decrees

No Bill Proposed

> The Federal Trade Commission's Bureau of Economics' (BE) role as an independent and expert analyst is one of the most critical features of the FTC's organizational structure in terms of enhancing its performance, expanding its substantive capabilities, and increasing the critical reputational capital the agency has available to promote its missions.[119]
>
> *Former FTC Commissioner Joshua Wright, 2015*

Commissioner Wright wrote as a veteran of both the Bureau of Economics and the Bureau of Competition. He was only the fourth economist to serve as FTC Commissioner (following Jim Miller, George Douglas and Dennis Yao) and the first JD/PhD. His 2015 speech, "On the FTC's Bureau of Economics, Independence, and Agency Performance," marked the beginning of an effort to bolster the role of the Bureau of Economics in the FTC's decision-making, especially in consumer protection matters. Wright warned, pointedly, that the FTC has "too many lawyers, too few economists," calling this "a potential threat to independence and agency performance."[120]

Unfortunately, this was only a beginning: shortly after delivering this speech, Wright resigned from the Commission to return to teaching law and economics. For now, at least, the task of bolstering economic analysis at the Commission falls to Congress.

The RECS Act's proposal that BE be involved in any recommendation for new legislation or regulatory action is an important step towards this goal, but it is too narrow.[121] It does not address the need to bolster the FTC's role in the institutional structure of the agency, or its role in enforcement decisions. The following chart (from Wright's speech) ably captures the first of these problems:

Number of Attorneys to Economists at the FTC from 2003 to 2013[122]

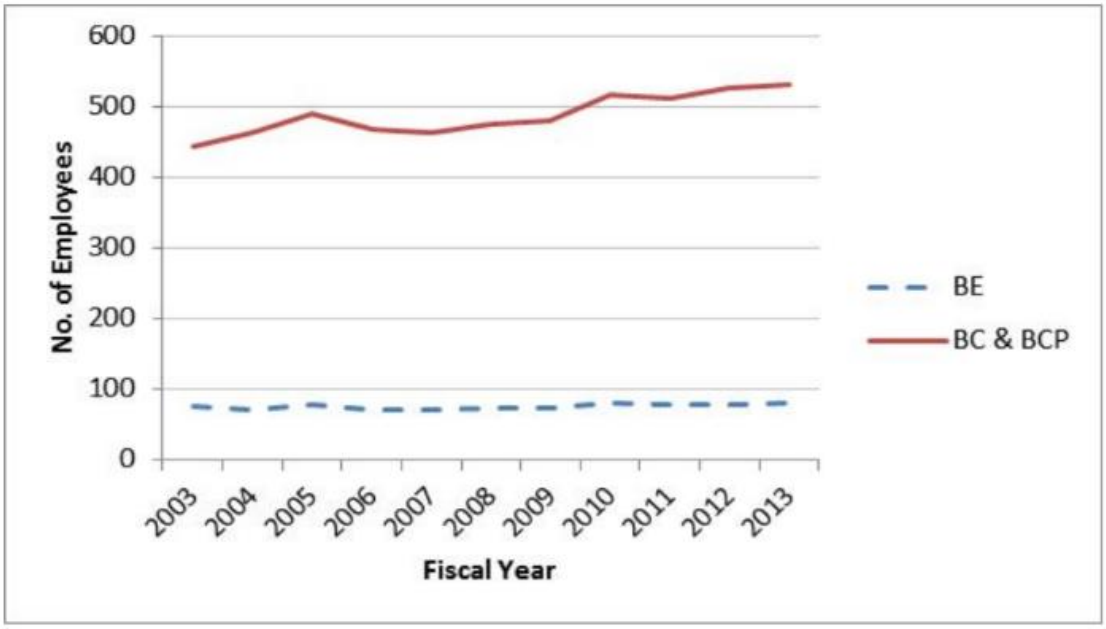
---

[119] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, at 1 (Aug. 6, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/695241/150806bestmtwright.pdf.

[120] *Id.* at 5.

[121] *See infra* at 54.

[122] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, *supra* note 119, at 6.



RECOMMENDATION: Hire More Economists

Wright recommends:

> Hiring more full-time economists is one obvious fix to the ratio problem. There are many benefits to expanding the economic capabilities of the agency. Many cases simply cannot be adequately staffed with one or two staff economists. **Doubling the current size of BE** would be a good start towards aligning the incentives of the Commission and BE staff with respect to case recommendations. While too quickly increasing the size of BE staff might dilute quality, a gradual increase in staffing coupled with a pay increase and a commitment to research time should help to keep quality levels at least constant.[123]

We wholeheartedly endorse former Commissioner Wright's recommendation.

RECOMMENDATION: Require BE to Comment Separately on Complaints and Consent Orders

In the case of complaints and consent orders issued by the Commission, we recommend that Congress require the Commission to amend its Rules of Practice to require that the Bureau of Economics provide a *separate* economic assessment of the complaint or consent order in conjunction with each. This proposal is consistent with former Commissioner Wright's similar recommendation:

---

[123] Statement of Commissioner Joshua D. Wright, On the FTC's Bureau of Economics, Independence, and Agency Performance, *supra* note 119, at 11.

> I suggest the FTC consider interpreting or amending FTC Rule of Practice 2.34 to mandate that BE publish, in matters involving consent decrees, and as part of the already required "explanation of the provisions of the order and the relief to be obtained," a separate explanation of the economic analysis of the Commission's action. The documents associated with this rule are critical for communicating the role that economic analysis plays in Commission decision-making in cases. In many cases, public facing documents surrounding consents in competition cases simply do not describe well or at all the economic analysis conducted by staff or upon which BE recommended the consent.[124]

In order to perform its desired function, this "separate explanation" would be authored and issued by the Bureau of Economics, and not subject to approval by the Commission. The document would express BE's independent assessment (approval or rejection) of the Commission's proposed complaint or consent order, provide a high-level description of the specific economic analyses and evidence relied upon in its own recommendation or rejection of the proposed consent order, and offer a more general economic rationale for its recommendation.

Requiring BE to make public its economic rationale for supporting or rejecting a complaint or consent decree voted out by the Commission would offer a number of benefits. In general, such an analysis would both inform the public and demand rigor of the Commission. As former Commissioner Wright noted,

> First, it offers BE a public avenue to communicate its findings to the public. Second, it reinforces the independent nature of the recommendation that BE offers. Third, it breaks the agency monopoly the FTC lawyers currently enjoy in terms of framing a particular matter to the public. The internal leverage BE gains by the ability to publish such a document… will also provide BE a greater role in the consent process and a mechanism to discipline consents that are not supported by sound economics…, minimizing the "compromise" recommendation that is most problematic in matters involving consent decrees.[125]

Wright explains this "compromise recommendation" problem in detail that bears extensive quotation and emphasis here:

> Both BC attorneys and BE staff are responsible for producing a recommendation memo. The asymmetry is at least partially a natural result of the different nature of the work that lawyers and economists do. But it is important to note that one consequence of this asymmetry, whatever its cause, is that it creates the potential to weaken BE's independence. BE maintains a high level of integrity and independence over core economic tasks – e.g., economic modeling and framing, statistical analyses, and assessments of outside economic work – yet when it comes

[124] *Id.* at 11-12.

[125] *Id.* at 11.

> to the actual policy recommendation, **I think it is fair to raise the question whether the Commission always receives unfiltered recommendations when BE dissents from the recommendation of BC or BCP staff.**
>
> One example of this phenomenon is the so-called "compromise recommendation," that is, a BE staff economist might recommend the FTC accept a consent decree rather than litigate or challenge a proposed merger when the underlying economic analysis reveals very little actual economic support for liability. In my experience, **it is not uncommon for a BE staff analysis to convincingly demonstrate that competitive harm is possible but unlikely, but for BE staff to recommend against litigation on those grounds, but in favor of a consent order**. The problem with this compromise approach is, of course, that a recommendation to enter into a consent order must also require economic evidence sufficient to give the Commission reason to believe that competitive harm is likely. This type of "compromise" recommendation in some ways reflects the reality of BE staff incentives. Engaging in a prolonged struggle over the issue of liability with BC and BC management is exceedingly difficult when the economist is simply outmanned. It also ties up already scarce BE resources on a matter that the parties are apparently "willing" to settle.[126]

The ability of BC or BCP staff to dilute the analysis of BE staffers in a combined compromise recommendation renders moot this provision of the operating manual:

> Dissenting staff recommendations regarding compulsory process, compliance, consent agreements, proposed trade regulation rules or proposed industrywide investigations should be submitted to the Commission by the originating offices, upon the request of the staff member.[127]

For this provision to have any effect, there must be a separate dissenting staff recommendation that can be seen by Commissioners — and, ideally, also made public.

RECOMMENDATION: Require BE to Comment on Upgrading Investigations

Similarly, we recommend enhancing BE's role earlier in the investigation process: at the point where the Bureau Director decides whether to upgrade an initial (Phase I) investigation to a full investigation. This is a critical inflection point in the FTC's investigative process for three reasons:

1. In principle, the staff is not supposed to negotiate consent decrees during the initial investigation phase;
2. In principle, the staff is not supposed to use compulsory discovery process during the initial investigation phase, meaning a target company's cooperation until this point is at least theoretically voluntary; and

---

[126] *Id.* at 7-8.

[127] Operating Manual § 3.3.5.1.1.

3. Either the decision to open a formal investigation or the subsequent issuance of CIDs may trigger a public company's duty to disclose the investigation in its quarterly securities filings.

It is also likely the point at which the staff determines (or at least begins to seriously consider) whether or not the Commission is likely to approve a staff recommendation to issue a complaint against any of the specific targets of the investigation.

For all these reasons, converting an initial investigation to a full investigation gives the staff enormous power to coerce a settlement. This decision deserves far more rigorous analysis than it currently seems to receive.

When the BC or BCP staff proposes to their Bureau director that an initial investigation be expanded into a full investigation, the FTC Operating Manual requires a (confidential) memorandum justifying a decision, but does *not* formally require the Bureau of Economics, or require that the analysis performed by any FTC staff correspond to two of the three requirements of Section 5(n) or the materiality requirement of the Deception Policy Statement:

> 3.5.1.4 Transmittal Memorandum
>
> The memorandum requesting approval for full investigation should clearly and succinctly explain the need for approval of the full investigation, including a discussion of relevant factors among the following:
>
> (1) A description of the practices and their impact on consumers and/or on the marketplace;
> (2) Marketing area and volume of business of the proposed respondent and the overall size of the market;
> (3) Extent of consumer injury inflicted by the practices to be investigated, the benefits to be achieved by the Commission action and/or the extent of competitive injury;
> (4) When applicable, an explanation of how the proposed investigation meets objectives and, where adopted, case selection criteria or the program to which it has been assigned;
> (5) When applicable, responses to the policy protocol questions (see OM Ch. 2);[128]

We recommend modifying this in two ways. First, while approving a complaint or a consent decree should absolutely require a separate recommendation from the Bureau of Economics, requiring such a recommendation merely to convert an initial investigation to a full investigation might well pose too great a burden on BE's already over-taxed resources. But that is no reason why the FTC rules should not at least give BE the *opportunity* to write a

[128] Operating Manual § 3.3.5.1.4 (emphasis added).

separate memorandum if it so desires. Having this written recommendation shared with Commissioners would serve as an early warning system, alerting them to potentially problematic cases being investigated by BCP or BC staff *before* the staff has extracted a consent decree — something that regularly has effectively happened by the time the Commission votes on whether to authorize a complaint. Thus, giving BE the opportunity to be involved at this early stage may be critical to scrutinizing the FTC's use of consent decrees.

Second, there is no reason that the memorandum prepared by either BC or BCP staff should not correspond to the doctrinal requirements of the relevant authority. The Operating Manual falls well short of this by merely requiring some analysis of the "[e]xtent of consumer injury." Why not countervailing benefit and reasonable avoidability, too, for Unfairness cases? And materiality in Deception cases? And the various other factors subsumed in the consumer welfare standard of the rule of reason, for Unfair Methods of Competition Cases?

That this would be only an *initial* analysis that will remain confidential under the Commission's rules is all the more reason it should not be a problem for the Staff to produce.

Economic Analysis in Reports & "Recommendations"

The Revealing Economic Conclusions for Suggestions (RECS) Act

Rep. Mike Pompeo's (R-KS) bill (H.R. 5136)[129] would require the FTC to include, in "any recommendations for legislative or regulatory action," analysis from the Bureau of Economics including:

> [T]he rationale for the Commission's determination that private markets or public institutions could not adequately address the issue, and that its recommended legislative or regulatory action is based on a reasoned determination that the benefits of the recommended action outweigh its costs.

Valuable as this is, the bill should be expanded to encompass other Commission pronouncements that aren't, strictly, "recommendations for legislative or regulatory action."

VALUE OF THE BILL: Bringing Rigor to FTC Reports, Testimony, etc.

The lack of economic analysis in support of "recommendations for legislative or regulatory action" has grown more acute with time — not only in the FTC's reports but also in its testimony to Congress.

Section 6(b) of the FTC Act gives the Commission the authority "to conduct wide-ranging economic studies that do not have a specific law enforcement purpose" and to require the

[129] The Revealing Economic Conclusions for Suggestions Act, H.R. 5136, 114th Cong. (2016) [hereinafter RECS Act] *available at* https://www.congress.gov/bill/114th-congress/house-bill/5136/text.

filing of "annual or special … reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of any company over which the FTC has jurisdiction, except insurance companies. This section is a useful tool for better understanding business practices, particularly those undergoing rapid technological change. But it is only as valuable as the quality of the analyses these 6(b) reports contain. And typically they are fairly short on economic analysis, especially concerning consumer protection matters.

The FTC has consistently failed to include any apparent, meaningful role for the Bureau of Economics in its consumer protection workshops or in the drafting of the subsequent reports. Nor has the FTC explored the adequacy of existing legal tools to address concerns raised by its reports. For example, the FTC's 2014 workshop, "Big Data: A Tool for Inclusion or Exclusion?," included not a single PhD economist or BE staffer.[130] The resulting 2016 report includes essentially just two footnotes on economics.[131] Commissioner Ohlhausen dissented, noting that

> Concerns about the effects of inaccurate data are certainly legitimate, but policymakers must evaluate such concerns in the larger context of the market and economic forces companies face. Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap….
>
> To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals. Today's report enriches the conversation about big data. My hope is that future participants in this conversation will test hypothetical harms with economic reasoning and empirical evidence.[132]

---

[130] Fed. Trade Comm'n, Public Workshop: Big Data: A Tool for Inclusion or Exclusion? (Sep. 15, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[131] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES FTC REPORT (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[132] *Id.* at A-1 to A-2.

The Commission's 2016 PrivacyCon conference did include several economists on a panel devoted to the "Economics of Privacy & Security."[133] But, as one of the event's discussants, Geoffrey Manne, noted:

> One of the things I would say is that it's a little bit unfortunate we don't have more economists and engineers talking to each other. As you might have gathered from the last panel, an economist will tell you that merely identifying a problem isn't a sufficient basis for regulating to solve it, nor does the existence of a possible solution mean that that solution should be mandated. And you really need to identify real harms rather than just inferring them, as James Cooper pointed out earlier. And we need to give some thought to self-help and reputation and competition as solutions before we start to intervene….
>
> So we've talked all day about privacy risks, biases in data, bad outcomes, problems, but we haven't talked enough about beneficial uses that these things may enable. So deriving policy prescriptions from these sort of lopsided discussions is really perilous.
>
> Now, there's an additional problem that we have in this forum as well, which is that the FTC has a tendency to find justification for enforcement decisions in things that are mentioned at workshops just like these. So that makes it doubly risky to be talking [] about these things without pointing out that there are important benefits here, and that the costs may not be as dramatic as it seems [just] because we're presenting these papers describing them.[134]

As Manne notes, as a practical matter, these workshops and reports are often used by the Commission either to make legislative recommendations or to define FTC enforcement policy by recommending industry best practices (which the agency will effectively enforce). But, again, because they lack much in the way of economically rigorous analysis, these recommendations may not be as well-founded as they may be presumed to be.

In its 2000 Report to Congress, for example, the FTC called for comprehensive baseline legislation on privacy and data security.[135] Congress has not passed such legislation, but the FTC repeated the recommendation in its 2012 Privacy Report.[136] While that Report called

---

[133] Fed. Trade Comm'n, *Conference: PrivacyCon* (Jan. 14, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon.

[134] Fed. Trade Comm'n, *Transcript of the Remarks of Geoffrey A. Manne*, 19 (Jan. 14, 2016), *available at* https://www.ftc.gov/system/files/documents/videos/privacycon-part-5/ftc_privacycon_-_transcript_segment_5.pdf#page=18.

[135] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

[136] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012), *available at*

(cont.)

for significantly stricter legislation, less tied to consumer harm, it did *not* include any economic analysis by the FTC's Bureau of Economics. Indeed, by rejecting the harms-based model of the 2000 Report,[137] the 2012 report essentially dismisses the *relevance* of economic analysis, either in the report itself or in case-by-case adjudication.

In his dissent, Commissioner Rosch warned about the Report's reliance on unfairness rather than deception, noting that "'Unfairness' is an elastic and elusive concept. What is "unfair" is in the eye of the beholder…."[138] In effect, Rosch, despite his long-standing hostility to economic analysis,[139] was really saying that the Commission had failed to justify its *analysis* of unfairness. Rosch objected to the Commission's invocation of unfairness against harms that have not been clearly analyzed:

> That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982 [sic], Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm. In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted.[140]

Rosch contrasted the Report's reliance on unfairness with the Commission's Unfair Methods of Competition doctrine, which he called "self-limiting" because it was tied to analysis of market power.[141] Rosch lamented that,

> There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world. That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n). I would instead stand by what we have said

---

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[137] PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, *supra* note 135.

[138] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE*, supra* note 136, at C-3.

[139] *See e.g.*, J. Thomas Rosch, *Litigating Merger Challenges: Lessons Learned* (June 2, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/litigating-merger-challenges-lessons-learned/080602litigatingmerger.pdf ("any kind of economic analyses that require the use of mathematical formulae are of little persuasive value in the courtroom setting;" "when I see an economic formula my eyes start to glaze over."); *See generally* Joshua Wright, *Commissioner Rosch v. Economics, Again*, TRUTH ON THE MARKET (Oct. 7, 2008), *available at* https://truthonthemarket.com/2008/10/07/commissioner-rosch-v-economics-again/.

[140] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at C-4.

[141] *Id.* at C-5.

> and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.[142]

The proposed bill would help to correct these defects, and to ensure that FTC Reports, at least those containing legislative or rulemaking recommendations, are based on the rigorous analysis that should be expected of an expert investigative agency's policymaking — especially one that has arguably the greatest pool of economic talent found anywhere in government in America.

RECOMMENDATION: Require Analysis of Recommended Industry Best Practices

In this regard the proposed bill would be enormously beneficial, but it could, and should, do significantly more.

First and foremost, the term "recommendations for legislative or regulatory action" would not encompass the most significant FTC recommendations: those included in "industry best practices" publications and reports produced by the Commission. These documents purport to offer expert suggestions for businesses to follow in order to help them to protect consumer welfare and to better comply with the relevant laws and regulations. But the FTC increasingly treats these recommendations as soft law, not merely helpful guidance, in at least two senses:

1. The FTC uses these recommendations as the basis for writing its 20-year consent-decree requirements, including ones unrelated, or only loosely related, to the conduct at issue in an enforcement action; and
2. The FTC uses these recommendations as the substantive basis for enforcement actions — for example, by pointing to a company's failure to do something the FTC recommended as evidence of the unreasonableness of its practices.

Former Chairman Tim Muris notes this about the "voluntary" guidelines issued by the FTC in 2009 in conjunction with three other federal agencies, comparing them to the FTC's efforts to ban advertising to children:

> The FTC has been down this road before. Prodded by consumer activists in the late 1970s, the Commission sought to stop advertising to children…
>
> One difference between the current proposal and the old rulemaking — called Kid Vid — is that this time the agencies are suggesting that the standards be adopted "voluntarily" by industry. Yet can standards suggested by a government

[142] *Id.*

> claiming the power to regulate truly be "voluntary"? Moreover, at the same workshop that the standards were announced, a representative of one of the same activist organizations that inspired the 1970s efforts speculated that a failure to comply with the new proposal would provoke calls for rules or legislation.[143]

Regulation by leering glare is still regulation.

Informed by the trauma of its near-fatal confrontation with Congress at the end of the Carter administration, the FTC was long skittish about making recommendations for businesses in its reports, beyond high level calls for attention to issues like data security. That changed in 2009, however. The FTC has since issued a flurry of reports recommending best practices like "privacy by design" and "security by design," first generally, and then across a variety of areas, from Big Data to facial recognition.[144]

The FTC's recommendations to industry in its 2005 report on file-sharing were admirably circumspect:

> Industry should decrease risks to consumers through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.[145]

This is not to say that the FTC could not or should not have done more to address the very real problem of inadvertent online file-sharing. Indeed, one of the authors of this report has lauded the (Democratic-led) FTC for bringing its 2011 enforcement action against Frostwire[146] for designing its peer-to-peer file-sharing software in a way that deceived users into unwittingly sharing files.[147] Rather, it is simply to say that the FTC, in 2005, understood that a report was not a substitute for a rulemaking — *i.e.*, not an appropriate place to make "recommendations" for the private sector that would have any force of law.

By 2012 the FTC had lost any such scruples. Its Privacy Report, issued that year, is entitled "Recommendations for Businesses and Policymakers." The title says it all: The FTC di-

---

[143] *Statement of Timothy J. Muris, supra* note 14, at 11-13.

[144] BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION, *supra* note 131; FED TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[145] FED. TRADE COMM'N, PEER-TO-PEER FILE-SHARING TECHNOLOGY: CONSUMER PROTECTION AND COMPETITION ISSUES (2005), *available at* https://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf.

[146] Fed. Trade Comm'n v. Frostwire LLC, FTC File No. 112 3041, https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon (2011).

[147] *Prepared Statement of Berin Szóka, President of TechFreedom: Hearing Before the H. Energy & Commerce Comm.* 112th Cong. (2012), 23, *available at* https://techliberation.com/wp-content/uploads/2012/11/Testimony_CMT_03.29.12_Szoka.pdf.

rected its sweeping recommendations for "privacy by design" to both the companies it regulates and the elected representatives the FTC supposedly serves:

> The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation.[148]

Of course, the FTC added:

> To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.[149]

Also noteworthy is the contrast between the two reports in their analytical rigor. The file sharing report noted:

> The workshop panelists and public comments did not provide a sufficient basis to conclude whether the degree of risk associated with P2P file-sharing programs is greater than, equal to, or less than the degree of risk when using other Internet technologies.[150]

The 2012 report shows no such modesty, as Commissioner Rosch lamented in his dissent ("There does not appear to be any such limiting principle applicable to many of the recommendations of the Report.").[151]

In 2015, Commissioner Wright expressed dismay at this same problem in his dissent from the staff report on the Internet of Things Workshop:

> I dissent from the Commission's decision to authorize the publication of staff's report on its Internet of Things workshop ("Workshop Report") because the Workshop Report includes a lengthy discussion of industry best practices and recommendations for broad-based privacy legislation without analytical support to establish the likelihood that those practices and recommendations, if adopted, would improve consumer welfare….
>
> First…, merely holding a workshop — without more — should rarely be the sole or even the primary basis for setting forth specific best practices or legislative recommendations….

---

[148] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at iii.

[149] *Id*. at vii.

[150] PEER-TO-PEER FILE-SHARING TECHNOLOGY, *supra* note 145, at 12.

[151] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 136, at C-5.

> Second, the Commission and our staff must actually engage in a rigorous cost-benefit analysis prior to disseminating best practices or legislative recommendations, given the real world consequences for the consumers we are obligated to protect….
>
> **The most significant drawback of the concepts of "security by design" and other privacy-related catchphrases is that they do not appear to contain any meaningful analytical content**…. An economic and evidence-based approach sensitive to [] tradeoffs is much more likely to result in consumer-welfare enhancing consumer protection regulation. To the extent concepts such as security by design or data minimization are endorsed at any cost — or without regard to whether the marginal cost of a particular decision exceeds its marginal benefits — then application of these principles will result in greater compliance costs without countervailing benefit. Such costs will be passed on to consumers in the form of higher prices or less useful products, as well as potentially deter competition and innovation among firms participating in the Internet of Things.[152]

The point illustrated by comparing these examples is the difficulty inherent in trying to require greater rigor from the FTC in recommendations to businesses when those recommendations can be either high level and commonsensical (as in 2005) or sweeping and effectively regulatory (as in 2012 and 2015). Thus, we recommend the following simple amendment to the proposed bill:

> [The FTC] shall not submit any ***proposed industry best practices, industry guidance or*** recommendations for legislative or regulatory action without [analysis]….

This wording would not apply to the kind of "recommendation" that the FTC made occasionally before 2009, as exemplified by the 2005 report. In any event, the bill's requirement is easily satisfied: essentially the FTC need only give the Bureau of Economics a role in drafting the report. Because this recommendation would not hamstring the FTC's enforcement actions, nor tie the FTC up in court, it should not be controversial, even if applied to proposed industry best practices and guidance.

Our proposed amendment would be simpler than attempting to broaden the definition of "regulatory action" beyond just rulemakings (which is how the FTC would likely limit its interpretation of the bill as drafted now) to include the kind of "regulatory action" that matters most: its use of reports to indicate how it will regulate through case by case enforcement, *i.e.*, its "common law of consent decrees."

---

[152] Dissenting Statement of Commissioner Joshua D. Wright, *Issuance of The Internet of Things: Privacy and Security in a Connected World Staff Report* (Jan. 27, 2015) (emphasis added), available at https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

RECOMMENDATION: Clarify the Bill's Language to Ensure It Applies to All FTC Reports

Another important difference between the 2000 and 2012 privacy reports is that the 2000 report is labelled "A Report to Congress," while the 2012 report is not and, indeed, barely mentions Congress. This reflects a little-noticed aspect of the way Section 6(f) is currently written, with subsection numbers added for clarity:

> (f) Publication of information; reports
>
> To [i] make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to [ii] make annual and special reports to the Congress and to submit therewith recommendations for additional legislation; and to [iii] provide for the publication of its reports and decisions in such form and manner as may be best adapted for public information and use.[153]

In other words, the Commission has shifted from relying upon 6(f)(ii) to 6(f)(i) and (iii). This distinction may seem unimportant, but it may cause the bill as drafted to be rendered meaningless, because the way it is worded could be read to apply only to 6(f)(ii). The bill would amend the existing proviso in Section 6(f) as follows:

> Provided [t]hat the Commission shall not submit any recommendations for legislative or regulatory action without an economic analysis by the Bureau of Economics….

The use of the words "submit" and "recommendations" clearly tie this proviso to 6(f)(ii). Thus, the FTC could claim that it need not include the analysis required by the bill unless it is specifically submitting recommendations to Congress, which it simply does not do anymore.

Instead we propose the following slight tweak to the bill's wording, to ensure that it would apply to the entirety of Section 6(f):

> Provided [t]hat the Commission shall not ***make*** any recommendations for legislative or regulatory action without an economic analysis by the Bureau of Economics…

This would require the participation of the Bureau of Economics in *all* FTC reports (that make qualifying recommendations), whatever their form. It would also require BE's participation in at least two other contexts where such recommendations are likely to be made: (i) Congressional testimony and (ii) the competition advocacy filings the Commission makes with state and local regulatory and legislative bodies, and with other federal regulatory

[153] 15 U.S.C. § 46(f)

agencies. This is a feature, not a bug: participation by BE is not something to be minimized; it should be woven into the fabric of *all* of the FTC's activities. As we have noted previously:

> The most important, most welfare-enhancing reform the FTC could undertake is to better incorporate sound economic- and evidence-based analysis in both its substantive decisions as well as in its process. While the FTC has a strong tradition of economics in its antitrust decision-making, its record in using economics in other areas is mixed.[154]

Because the bill does not in any way create a cause of action against the FTC for failing to comply with the requirement, it will not hamstring the FTC if the agency fails to take the bill's requirements seriously. That, if anything, is a weakness of the bill, but it is largely inevitable. It will always be up to the discretion of the Commission itself (subject, of course, to congressional oversight) to decide how much "economic analysis" is "sufficient" under the bill.

RECOMMENDATION: Require a Supermajority of Commissioners to Decide What Analysis is "Sufficient"

As written, the bill might do little more than shame the Chairman into involving the Bureau of Economics somewhat more in the writing of reports and the workshops that lead to them — if only because the bill might embolden a single Commissioner to object to the FTC's lack of analysis, as Commissioner Wright objected to the FTC's Internet of Things report.[155] This change in incentives for the Chairman and other commissioners, alone, may not significantly improve the analytical quality of the FTC's reports, given the hostility of the Bureau of Consumer Protection to economic analysis, although having *any* involvement by BE would certainly be an improvement.

Again, the question of "sufficiency" is inherently something that will be left to the Commission's discretion, but there is no principled reason that it has to be resolved through simple majority votes. On the other hand, giving a single Commissioner the right to veto an FTC "recommendation" as lacking a "sufficient" analytical basis might go too far.

We recommend striking a balance by requiring a supermajority (majority plus one, except in the case of a three-member Commission) of Commissioners to approve of the sufficiency of the analysis — essentially that this vote be taken, or at least recorded, separately from the vote on the issuance of the report itself. (The "sufficiency" vote would not stop the FTC from issuing a report.) At the same time, we recommend that the outcome of the "sufficien-

---

[154] Geoffrey A. Manne, *Humility, Institutional Constraints and Economic Rigor: Limiting the FTC's Discretion*, ICLE White Paper 2014-1 (Feb. 28, 2014) at 4, *available at* http://docs.house.gov/meetings/IF/IF17/20140228/101812/HHRG-113-IF17-Wstate-ManneG-20140228-SD002.pdf.

[155] *See Issuance of The Internet of Things: Privacy and Security in a Connected World Staff Report*, *supra* note 152, at 4.

cy" vote be disclosed on the first page of all reports or other documents containing recommendations.

Such a mechanism would effectively expand the set of options for which Commissioners could vote, enabling them to express subtler degrees of preference without constraining them, as now, into making the binary choice between approving or rejecting a recommendation *in toto*. In other words, while the cost of expressing disapproval today, in the form of a dissent from a report, may be too high in some cases (especially for Commissioners in the majority party), the cost of expressing disapproval for the sufficiency of analysis without vetoing an entire report would be much lower. Allowing such a vote, and publishing its results, would offer important information to the public. It would also increase the leverage of commissioners most concerned with ensuring that FTC recommendations are supported by sufficient rigor to influence the content and conclusions of FTC reports and similar documents.

In cases where the three-member majority feels the two-member minority's objections to analytical rigor are merely a pretense for objections to the recommendations themselves, the bill as we envision it would do nothing to stop the majority from issuing its recommendations anyway, of course; the "sufficiency" vote in this sense may sometimes be merely an expression of preference. Nonetheless, the majority Commissioners would likely be compelled to do more to explain why they believe the analysis included in support of a recommendation is sufficient, and why the minority is conflating its own policy views with the question of analytical sufficiency. These would also be valuable additions to the public's understanding of the basis for Commission recommendations

The virtue of our proposed approach is that it would further lower the bar for the Commission to do something it ought to do anyway: involve the Bureau of Economics in its decision-making.

RECOMMENDATION: Codify Congress's Commitment to Competition Advocacy

As we propose amending the RECS Act, consistent with the spirit with which we believe the bill is intended, BE would also have to be involved in any competition advocacy filings made by the FTC. Again, we believe this is all for the good. But it might, on the margin, discourage the FTC from issuing such filings in the first place — something we believe the FTC already does not do enough of. Thus, as discussed below, we recommend that Congress do more to encourage competition advocacy filings by the FTC.[156] At minimum, this means amending Section 6 to provide specific statutory authority for competition advocacy, something the FTC only vaguely divines from the Section today. As the text stands today, this authority is far from apparent, especially because the current Section 6 makes reference

[156] *See infra* note 87.

to "recommendations" only with respect to *Congress* in what we above refer to as Section 6(f)(ii).

Other Sources of Enforcement Authority (Guidelines, etc.)

The Solidifying Habitual & Institutional Explanations of Liability & Defenses (SHIELD) Act

Rep. Mike Pompeo's (R-KS) bill (H.R. 5118)[157] clarifies what is already black letter law: agency guidelines do not create any binding legal obligations, either upon regulated companies or the FTC. This means the FTC can bring enforcement actions outside the bounds of its Unfairness and Deception Policy Statements, its Unfair Methods of Competition Enforcement Policy Statement, and its regulations promulgated under other statutes enforced by the Commission (*e.g.*, the "Safeguards Rule," promulgated under the Gramm-Leach-Bliley Act)[158] unless Congress codifies the Statements in the statute. The only substantively operative provision of the bill is section (B), which provides that:

> Compliance with any guidelines, general statement of policy, or similar guidance issued by the Commission may be used as evidence of compliance with the provision of law under which the guidelines, general statement of policy, or guidance was issued.

This does not create a formal safe harbor; it merely allows companies targeted by the FTC to cite FTC's past guidance in their defense. This should be uncontroversial.

VALUE OF THE BILL: Increasing Legal Certainty and Decreasing the Coercive Regulatory Effect of the FTC's Soft Law

The bill would accomplish two primary goals. First, it would formally bar the FTC from doing something it has likely been doing in practice for some time: treating its own informal guidance as quasi-regulatory. To the extent that the Commission actually does so, it would effectively be circumventing the safeguards Congress imposed in 1980 upon the FTC's Section 5 rulemaking powers by amending the FTC Improvement Act of 1975 (commonly called "Magnuson-Moss").[159] But of course, for exactly this reason, the Commission would

---

[157] Solidifying Habitual and Institutional Explanations of Liability and Defenses Act, H.R. 5118, 114th Cong. (2016) [hereinafter SHIELD Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5118/text.

[158] Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

[159] The term Magnuson-Moss is inapt for two reasons. First, as former Chairman Muris explains, "Although within the Commission these procedures are uniformly referred to as 'Magnuson Moss,' in fact, the procedures are contained within Title II of the Magnuson Moss Warranty–Federal Trade Commission Improvement Act of 1975. Only Title I involved the Magnuson Moss Warranty Act…" *Statement of Timothy J. Muris*, *supra* note

(cont.)

never *admit* that this is what it is doing when its enforcement agenda just happens to line up with its previous recommendations.

More clear and more troubling is that, in the *LabMD* case, the Commission argued that the company, a small cancer testing lab, had committed an unfair trade practice sometime between 2006 and 2008 by failing to take "reasonable" measures to prevent the installation and operation of peer-to-peer file-sharing software on its network, which made patient billing information accessible to Tiversa, a company with specialized tools capable of scouring P2P networks for sensitive information. Crucial to the FTC's Complaint was its allegation that:

> Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.[160]

The Commission was referring, obliquely, to its 2005 report,[161] which offered this rather unhelpful suggestion to affected companies:

> Industry should decrease risks to consumers through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.

Not until January 2010 did the FTC issue "Peer-to-Peer File Sharing: A Guide for Business"[162] — about the same time, it appears, that the FTC undertook its investigation of LabMD. The SHIELD Act would clearly bar the FTC from pointing to its own past guidance as creating a legal trigger for liability. The Commission's assessment of "reasonableness" would have to be proven through other factors; indeed, since "reasonable" is found nowhere in Section 5 or even in the Unfairness Policy Statement, the Commission would have to prove the underlying elements of unfairness, without shortcutting this analysis by oblique reference to its own past reports.

A related concern is the Commission's application of rules promulgated in one context, in which they have binding authority, to other contexts in which they do not. The most striking example of this practice is the Commission's use of the Safeguards Rule, which "applies to the handling of customer information by all financial institutions over which the [FTC]

14, at 22, n. 44. Second, the safeguards at issue were adopted in 1980, not 1975, when "Mag-Moss" was passed.

[160] Complaint, In the Matter of LabMD, Inc., Docket No. 9357 at 4, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

[161] PEER-TO-PEER FILE-SHARING TECHNOLOGY, *supra* note 145.

[162] Fed. Trade, Comm'n, *Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business.

has jurisdiction,"[163] to define unfair data security practices, and the remedies applied by the FTC in consent decrees, outside the financial sector. Although the Safeguards Rule has regulatory authority for financial institutions, its authority is no different than informal guidance (or recommended "best practices") the Commission offers for everyone else. Nevertheless, the Commission has imposed remedies virtually identical to the Safeguards Rule in nearly every data security consent order into which it has entered.

> [T]he majority of the FTC's [data security] cases, regardless of cause of action or facts, impose the same remedy: the set of security standards laid out in the FTC's Safeguards Rule. Most notably, this is true regardless of whether the respondents were financial institutions (to which the Safeguards Rule directly applies) or not (to which the Rule has no direct application), and regardless of whether the claim is generally one of deception or unfairness.[164]

Second, the SHIELD Act would allow companies to raise their compliance with FTC guidance as part of their defense. This would, at a minimum, help encourage companies to resist settling legally questionable or analytically unsupported enforcement actions.

RECOMMENDATION: Clarify that Consent Decrees, Reports, and FTC Best Practices are not Binding

We propose expanding the bill's language slightly to ensure that it achieves its intended goal:

> No guidelines, general statements of policy, ***consent decrees, settlements, reports, recommended best practices***, or similar guidance issued by the Commission shall confer any right.

As should be clear by now, these other forms of soft law are the most important aspects of the FTC's discretionary model, especially given the paucity of policy statements (building upon the three major ones, such as on materiality, for example) or issue-specific "Guides."

Specifically, the Commission regularly applies its recommended best practices (grouped under catchphrases like "privacy by design" and "security by design") as mandatory company-specific regulations in consent decrees that are themselves applied, in cookie-cutter fashion, across enforcement actions brought against companies that differ greatly in their circumstances, and regardless of the nature or extent of the injury or the specific facts of their case.

Second, the *LabMD* case provides at least one clear example wherein the FTC has treated its own previous reports, making vague recommendations about the need for better industry data security practices (regarding peer-to-peer file-sharing), as a critical part of the trigger for

---

[163] 16 C.F.R. § 314.1(b).

[164] Manne & Sperry, *supra* note 52, at 20.

legal liability.[165] We suspect this is the tip of the iceberg — that the FTC in fact does this kind of thing quite often, but usually does not have to admit it, because it is able to settle cases without revealing its legal arguments. Only in the *LabMD* case (one of the first (of two) data security cases to be litigated after more than a decade of FTC consent decrees in this area) did the Commission have to make the connection between its previous "recommendations" and its application of Section 5. Even here, in its *LabMD* Complaint, it should be noted, the Commission did not specifically cite its 2005 P2P file-sharing report, but instead vaguely alluded to it — suggesting that even FTC staff were wary of revealing this connection.

RECOMMENDATION: Specify When a Defendant May Raise Evidence of Its Compliance with FTC Guidance

The bill does not currently specify *when* in the enforcement process evidence of compliance may be cited. It is important that a defendant be able to raise a compliance defense as early as possible. Without such an opportunity, the Commission can drag out an investigation that should have been terminated early, as when the subject of the investigation acted in good faith reliance upon the Commission's own statements. Ideally, this would occur during motions to quash CIDs.

Further, it would help if the FTC amended its rule on such motions, 16 C.F.R. § 2.10, to specify that this defense could be raised at part of a motion to quash. And, as we noted above,[166] it is critical that these challenges be permitted to remain confidential, as many companies may choose to avoid the risk the public exposure that comes with challenging CIDs.

At a minimum, the defendant should be able to raise this defense in a way that is communicated to Commissioners *before* the Commission's vote on whether to issue a complaint.

RECOMMENDATION: Encourage the FTC to Issue More Policy Statements & Guides

As the proposed SHIELD Act reflects, while there is some risk of ossification from over-reliance on *ex ante* guidelines and policy statements, the absence of such guidance documents can leave consumers and economic actors with insufficient notice of FTC enforcement principles and practices. Absent meaningful constraints on the Commission's discretionary authority, the costs of over-enforcement may be as great or greater than the costs of over-regulation. For these reasons, the bill should require the FTC to issue substantive

---

[165] *See supra* note 66 and note 161.

[166] *See supra* at 46.

guidelines, allow private parties to petition the FTC to issue guidelines, or allow a single Commissioner to force the issue.

A good place to start would be privacy regulation, where the Commission has issued no meaningful guides.[167] The Commission has done better on data security, with guides, for example, on photocopier data security (2010),[168] P2P software (2010),[169] and mobile app security (2013).[170] But none of these, and even the particularly thorough "Start with Security: A Guide for Business" (2015),[171] does the kind of thing the various antitrust guidelines do: expand upon the *analytical framework* by which the Commission determines how much security is enough. This must be grounded in the component elements of Section 5, not the Commission's policy agenda or technical expertise.

More important than issue-specific guides would be guidance one step up the Doctrinal Pyramid, explaining how concepts like materiality, weighing injury with benefits, and measuring reasonable avoidability will be measured.[172] Such a document would greatly enhance the value of issue-specific guides by allowing regulated companies to understand not just what the Commission might demand in the future, but the doctrinal legal basis for doing so.

Remedies

Appropriate Tailoring of Remedies

No Bill Proposed

The FTC has, perhaps predictably, also pushed the envelope with regard to the sorts of remedies it seeks against a broader category of targets. Initially, the Commission was given authority to pursue permanent injunctions under Section 13(b) as part of its ongoing mission to curb outright fraud.[173] Over time, however, the FTC has expanded its use of Section 13(b)

---

[167] See, e.g., Fed. Trade Comm'n, *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks* (Dec. 2012), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor

[168] Fed. Trade Comm'n, *Copier Data Security: A Guide for Businesses* (Nov. 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/copier-data-security-guide-businesses

[169] *Peer-to-Peer File Sharing: A Guide for Business*, *supra* note 162.

[170] Fed. Trade Comm'n, *Mobile App Developers: Start with Security* (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security

[171] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (Jun. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[172] *See supra* note 12.

[173] *See generally* Beales & Muris, *supra* note 21.

in order to target companies that engage in conduct that implicates issues from substantiation claims to product design — all far from fraudulent territory.[174]

For instance, Apple, Google, and Amazon have all been targets of the Commission for issues related to the design and function of their respective mobile app stores.[175] Amazon, one of the rare parties to proceed to full litigation on a Section 5 unfairness case, recently lost a summary judgment motion on a claim that its in-app purchasing system permitted children to make in-app purchases without parental "informed consent," thus engaging in an "unfair practice."[176] As part of its case the Commission sought a permanent injunction under Section 13(b) against Amazon on the basis of the Commission's claim that it was "likely to continue to injure consumers, reap unjust enrichment, and harm the public interest."[177]

This practice, called "fencing-in,"[178] may be appropriate for the inveterate fraudsters — against whom it is authorized under Section 19 of the Act:

> If the Commission satisfies the court that the act or practice to which the cease and desist order relates is **one which a reasonable man would have known under the circumstances was dishonest or fraudulent**, the court may grant… such relief as the court finds necessary.[179]

The FTC — in the past — indeed viewed Section 13(b) as a tool to police clearly fraudulent practices. "Consistent with the limitations in Section 19, the agency used Section 13(b) for a narrow class of cases involving fraud, near fraud, or worthless products."[180] Meanwhile, courts, for their part, "blessed this limited expansion of FTC authority," and still see the appropriate scope of Section 13(b) as a limited one.

---

[174] *Id.* at 4.

[175] *See* Geoffrey A. Manne, *Federal Intrusion: Too Many Apps for That*, WALL STR. J. (Sep. 16, 2014), http://www.wsj.com/articles/geoffrey-manne-federal-intrusion-too-many-apps-for-that-1410908397.

[176] Fed. Trade Comm'n v. Amazon.com, Inc., Case No. C14-1038-JCC, slip op. at 10 (W.D. Wash 2016), available at https://www.ftc.gov/system/files/documents/cases/160427amazonorder.pdf.

[177] *Id.* at 10.

[178] *See, e.g.*, Federal Trade Commission V. RCA Credit Services, LLC, Case No. 8:08-CV-2062-T-27AEP. (M.D. Fla. Jul 21, 2010) at 20 ("Courts also have discretion to include 'fencing-in' provisions that extend beyond the specific violations at issue in the case to prevent Defendants from engaging in similar deceptive practices in the future.").

[179] 15 U.S.C. § 57(b)-(a)(2) and -(b).

[180] Beales & Muris, *supra* note 21, at 22.

But the argument for extending fencing-in beyond the fraud context is extremely weak. Nevertheless, the FTC has more recently, as in the *Amazon* case, sought to use 13(b) against legitimate companies, dramatically expanding its scope — and its *in terrorem* effect.[181]

> Such broad "fencing in" relief (imposition of behavioral requirements that are more extensive than required [in order] to avoid future violations) goes well beyond prior FTC practice and may be aimed at "encouraging" other firms in similar industries to adopt costly new testing.[182]

Effectively, from the Commission's perspective, Amazon — with its app store that satisfied the needs of a huge number of consumers — was legally equivalent to "defendants engaged in continuous, fraudulent practices [who] were deemed likely to reoffend based on the 'systemic nature' of their misrepresentations."[183] This could not have been what Congress intended.

The courts, when they are presented with the opportunity to review this approach (as they sometimes are in Deception cases and as they virtually never are in Unfairness cases, given the lack of litigation) have been less than receptive. Although Amazon lost its motion for summary judgment, it prevailed on the question of whether Section 13(b) presented an appropriate remedy for its alleged infractions.

> While permanent injunctions are often awarded in cases where liability under the FTC Act is determined, Amazon correctly distinguishes those cases from the facts of this case… [C]ases in which a permanent injunction has been entered involved deceptive, ongoing practices.[184]

The court properly noted that it was incumbent upon the Commission to "establish, with evidence, a cognizable danger of a recurring violation."[185]

Similarly, in *FTC v. RCA Credit* (a Deception case), the court rejected the FTC's use of 13(b) — in that case, accepting the permanent injunction but questioning the expansion of its scope:

> The undisputed facts demonstrate that this is a proper case for permanent injunctive relief. However, the Court will defer ruling on the appropriate scope of an injunction (including whether, as the FTC requests, the injunction should include a

---

[181] *Id.* at 4 ("The FTC now threatens to expand the use of the Section 13(b) program beyond fraud cases, suggesting that it may use Section 13(b) to seek consumer redress even against legitimate companies.").

[182] Alden Abbott, *Time to Reform FTC Advertising Regulation*, Heritage Foundation Legal Memorandum #140 on Regulation (Oct. 29, 2014), *available at* http://www.heritage.org/research/reports/2014/10/time-to-reform-ftc-advertising-regulation#_ftnref21.

[183] Amazon case at 11.

[184] Amazon case at 11.

[185] *Id.* at 11.

> broad fencing-in provision enjoining misrepresentations of material fact in connection with the sale of any goods and services) until after hearing evidence on the issue.[186]

The reluctance of some courts to abet the FTC's expansion of its use of fencing-in remedies to reach legitimate companies is reassuring — and affirms our belief as to what Congress intended in Section 13(b). Unfortunately, however, most parties do not proceed to ruinously expensive litigation with the Commission, and will accede to the demands of a consent order. This creates undue costs of both the first order (companies agreeing to remedies that are larger or more invasive than what a court would impose) and the second order (the systemic cost of companies settling cases they might otherwise litigate, all regulated entities losing the benefit of litigation, and the FTC having to do less rigorous analysis).

The FTC's ability to threaten a permanent injunction, or to dramatically extend its scope beyond the practices at issue in a case, gives parties an inefficiently large incentive to settle in order to avoid the risk of the more draconian remedy. But, in doing so, parties end up opting in to consent orders that allow the FTC to evade any judicially enforced limits on the remedies it imposes, which is what the Commission *really* wants. Whatever the benefits to the agency from permanent injunctions, it arguably receives even more benefit from the ability to impose more detailed behavioral remedies than a court might permit (and to do so in the context of a consent order, the violation of which is subject to the lower burden of proving contempt rather than an initial violation).

The Commission's general resistance to constraints upon its remedial discretion was aptly illustrated by its abrupt revocation, in 2012,[187] of its 2003 Policy Statement On Monetary Equitable Remedies in Competition Cases (commonly called the Disgorgement Policy Statement).[188] As Commissioner Ohlhausen noted in her dissent from the withdrawal of the policy:

> Rescinding the bipartisan Policy Statement signals that the Commission will be seeking disgorgement in circumstances in which the three-part test heretofore utilized under the Statement is not met, such as where the alleged antitrust violation

---

[186] RCA Credit case at 24.

[187] Fed. Trade Comm'n, *FTC Withdraws Agency's Policy Statement on Monetary Remedies in Competition Cases; Will Rely on Existing Law* (Jul. 31, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies.

[188] Fed. Trade Comm'n, Policy Statement On Monetary Equitable Remedies — Including in Particular Disgorgement and Restitution, in FEDERAL TRADE COMMISSION COMPETITION CASES ADDRESSING VIOLATIONS OF THE FTC ACT, THE CLAYTON ACT, OR THE HART-SCOTT-RODINO ACT (2003), *available at* https://www.ftc.gov/public-statements/2003/07/policy-statement-monetary-equitable-remedies-including-particular.

> is not clear or where other remedies would be sufficient to address the violation.[189]

Not only does this mean that parties in general are more likely to settle, but it also means that parties that are facing novel, untested antitrust theories are more likely to settle. This allows the Commission to expand its antitrust enforcement authority beyond judicially recognized conduct without risk of reversal by the courts.

Section 13(b) and the Commission's disgorgement powers represent tremendous weapons to wield over the heads of investigative targets. Their expanding use to impose expansive or draconian remedies in cases involving non-fraudulent, legitimate companies and questionable legal theories is extremely troubling. Not only is this bad policy, it is also inconsistent with the spirit of the FTC Act, which was designed to find and punish actively fraudulent conduct, and to deter anticompetitive behavior that is not countervailed by pro-consumer benefits. But most of all, this gives the FTC greater ability to coerce companies that might otherwise litigate into settlements, pushing us further away from the Evolutionary Model and towards the Discretionary Model.

To correct these problems, at least two things should be done:

RECOMMENDATION: Limit Injunctions to the "Proper Cases" Intended by Congress

First, the Commission's use of Section 13(b) remedies should be reevaluated in light of the law's original purpose:

> [O]ne class of cases clearly improper for awarding redress under Section 13(b): traditional substantiation cases, which typically involve established businesses selling products with substantial value beyond the claims at issue and disputes over scientific details with well-regarded experts on both sides of the issue. In such cases, the defendant would not have known ex ante that its conduct was "dishonest or fraudulent." Limiting the availability of consumer redress under Section 13(b) to cases consistent with the Section 19 standard strikes the balance Congress thought necessary and ensures that the FTC's actions benefit those that it is their mission to protect: the general public.[190]

---

[189] Dissenting Statement of Commissioner Maureen K. Ohlhausen, *Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases* (Jul. 31, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120731ohlhausenstatement.pdf.

[190] Beales & Muris, *Striking the Proper Balance*, *supra* note 21, at 6.

[190] 15 U.S.C. § 57(b)-(a)(2) and -(b).

[190] Beales & Muris, *Striking the Proper Balance*, *supra* note 21, at 6–7.

This same logic applies to a host of other types of cases, as well, including the Commission's recent product design cases.[191] Thus the tailoring of the Commission's Section 13(b) powers should not stop merely with substantiation cases, but should extend, as a general principle, to any party that had not intentionally or recklessly engaged in conduct it should have known was dishonest or fraudulent. As Josh Wright noted in his dissent in the Apple product design case:

> The economic consequences of the allegedly unfair act or practice in this case — a product design decision that benefits some consumers and harms others — also differ significantly from those in the Commission's previous unfairness cases.
>
> The Commission commonly brings unfairness cases alleging failure to obtain express informed consent. These cases invariably involve conduct where the defendant has intentionally obscured the fact that consumers would be billed. Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud — the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items. Under this scenario, the allegedly unfair act or practice injures consumers and does not provide economic value to consumers or competition. In such cases, the requirement to provide adequate disclosure itself does not cause significant harmful effects and can be satisfied at low cost.
>
> However, the particular facts of this case differ in several respects from the above scenario.[192]

The same logic that undergirds former Commissioner Wright's objection to the majority's aggressive application of the UPS in *Apple* applies equally to the aggressive 13(b) remedies sought in similar cases.

RECOMMENDATION: Narrow Overly Broad "Fencing-in" Remedies

Similarly, the imposition of unreasonable behavioral demands — "fencing-in" of conduct beyond that at issue in the case — upon parties subject to FTC enforcement is problematic.

---

[191] Fed. Trade Comm'n, *FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges* (Jul. 10, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars; In the Matter of Apple Inc., FTC File No 112 3108, https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc (2014); Fed. Trade Comm'n, *Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges* (Sept. 4, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it.

[192] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 3 (Jan. 15, 2014), *available at* https://goo.gl/0RCC9E.

.

For instance, in *Fanning v. FTC*, the Commission imposed upon defendant John Fanning a requirement that the First Circuit characterized as "not reasonably related to [the alleged] violation."[193] In 2009, Fanning founded jerk.com, a social networking website that controversially enabled users to nominate certain persons to be "jerks."[194] In issuing a variety of challenges to jerk.com's business practices — including an alleged failure of the site to facilitate paid customers' removal of negative information — the Commission additionally applied a "compliance monitoring" provision aimed directly at Fanning.[195] This provision required that Fanning "notify the Commission of… his affiliation with any new business or employment," and submit information including the new business's "address and telephone number and a description of the nature of the business" for a period of ten years.[196] Under the Commission's cease and desist order, it did not matter whether Fanning engaged in reputation work, or started social media sites, or not — the requirement applied regardless of what type of work Fanning did and for whom he did it.[197]

The First Circuit rebuked the Commission on this point:

> When asked at oral argument, the Commission conceded that this provision would ostensibly require Fanning to report if he was a waiter at a restaurant. The only explanation offered by the Commission for this breadth is that it has traditionally required such reporting.[198]

Moreover, the Commission cited a string of district court cases upholding similar provisions which the court characterized as "almost entirely bereft of analysis that might explain the rationale for such a requirement."[199] While it is encouraging that the First Circuit saw fit to rein in the Commission, it is also apparent that the FTC frequently receives an extraordinary degree of deference from district courts, even when creating punitive provisions that bear little or no connection to challenged subject matter.

In order to deter the Commission from taking advantage of this frequent judicial deference by imposing such disconnected "fencing-in" remedies in non-fraud cases — which, of course, is compounded by the fact that most cases are never reviewed by courts at all — Congress should consider imposing some sort of minimal requirement that provisions in

---

[193] Fanning v. Fed. Trade Comm'n, FTC File No. 15-1520, slip op. at 13 (May 9, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/051816jerkopinion.pdf.

[194] *Id.* at 2-3.

[195] *Id.* at 21-22.

[196] *Id.* at 22.

[197] Final Order, Fanning v. Fed. Trade Comm'n, FTC File No. 15-1520 (March 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150325jerkorder.pdf

[198] *Id.* at 23-24.

[199] *Id.* at 24.

proposed orders and consent decrees be (i) reasonably related to challenged behavior, and (ii) no more onerous than necessary to correct or prevent the challenged violation.

This reform is also important to minimizing the daisy-chaining of consent decrees discussed in the next Section.[200] As we note there, the ability of the Commission to bring a second enforcement action not premised on Section 5, but rather on the terms of a consent decree that is vaguely related to the challenged conduct creates several problems. The Commission's ability to do this is magnified if the initial consent order already contains provisions that reach a broad range of conduct or that include a host of difficult conduct remedies that the company may even inadvertently violate.

RECOMMENDATION: Revive the 2003 Disgorgement Policy

Second, Congress should consider requiring the Commission to return to its previous disgorgement policy, or to propose targeted amendments to it. At a minimum, the Commission should be required to perform *some* process to examine the issue and take public comment on it. As Commissioner Ohlhausen noted in her dissent, objecting to the vote to rescind the Policy Statement:

> I am troubled by the seeming lack of deliberation that has accompanied the withdrawal of the Policy Statement. Notably, the Commission sought public comment on a draft of the Policy Statement before it was adopted. That public comment process was not pursued in connection with the withdrawal of the statement. I believe there should have been more internal deliberation and likely public input before the Commission withdrew a policy statement that appears to have served this agency well over the past nine years.[201]

Consent Decree Duration & Scope

The Technological Innovation through Modernizing Enforcement (TIME) Act

Subcommittee Chairman Rep. Michael C. Burgess, M.D.'s (R-TX) bill (H.R. 5093)[202] would, in non-fraud cases, limit FTC consent orders to eight years — instead of the 20 years the FTC usually imposes. If the term runs five years or more, the FTC must reassess the decree after five years under the same factors required for setting the length of the consent decree from the outset:

---

[200] *See infra* at 76.

[201] *Id.* at 2.

[202] The Technological Innovation through Modernizing Enforcement Act, H.R. 5118, 114th Cong. (2016) [hereinafter TIME Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5093/text.

1. The impact of technological progress on the continuing relevance of the consent order.
2. Whether there is reason to believe that the entity would engage in activities that violate this section without the consent order 8 years after the consent order is entered into by the Commission.

Shortening the length of consent decrees will do much to address the abuse of consent decrees, but it will not fix the underlying problems, as we discuss below.

VALUE OF THE BILL: Reducing the Abuse of Consent Decrees as *De Facto* Regulations

This reform is critical to reducing the FTC's use of consent decrees as effectively regulatory tools. It is entire commonplace for the FTC to impose the same twenty-year consent decree term and the same conditions (drawn from its quasi-regulatory reports) on every company, regardless of the facts of the case, the size of the company etc. Limiting the duration of consent decrees would not entirely stop abuse of consent decrees as a way to circumvent Section 5 rulemaking safeguards (because each consent decree is effectively a mini-rulemaking, which implements the FTC's pre-determined policy agenda), but it would at least limit the damage, and clear overly broad consent decrees more quickly.

The bill would also make it less likely that the FTC could daisy-chain additional enforcement actions — that is, bring a second enforcement action not premised on Section 5 (and therefore not even paying lip service to its requirements) but on the terms of a consent decree that is only vaguely related to the subsequent conduct. Such daisy-chaining has allowed enormous leverage in forcing settlements, since the FTC Act gives the Commission civil penalty authority only for violations of consent decrees (and rules), not Section 5 itself. Thus, the FTC gains the sledgehammer of potentially substantial monetary fines the second time around. It also allows the FTC to further extend the term of the consent decree beyond the initial 20 years — and potentially keep a company operating under a consent decree forever.

This is essentially what the FTC did to Google. First, in 2011, the FTC and Google settled charges that Google had committed an unfair trade practice in 2010 in by opting Gmail users into certain features of its new (and later discontinued) Buzz social network.[203] A year later, the FTC imposed a $22.5 million penalty against Google in settling charges that Google had violated the 2011 consent decree by misleading consumers by, essentially, failing to update an online help page that told users of Apple's Safari browser that they did not need to take further action to avoid being tracked, after a technical change made *by Apple*

[203] Fed. Trade Comm'n, *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Networ*k (Mar. 30, 2011), available at https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

had rendered this statement untrue.[204] The FTC's Press Release boasted "Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order."[205] The case raised major questions about the way the FTC understood its deception authority,[206] none of which were dismissed because (a) Google, already being under the FTC's thumb and facing a potentially even-larger monetary penalty, was eager to settle the case, and (b) the FTC technically did not have to prove the normal elements of deception, such as the materiality of a help page seen by a tiny number of users, because it was enforcing the consent decree, not Section 5.

Perhaps most disconcertingly, the Commission's 2012 action against Google had precious little to do with the conduct that gave rise to its 2011 consent order. To be sure, the 2011 order was written in the broadest possible terms, arguably covering nearly every conceivable aspect of Google's business. But this just underscores the regulation-like nature of the Commission's consent orders, as well as the FTC's propensity to treat cases with dissimilar facts and dissimilar circumstances essentially the same. While that kind of result might be expected of a regulatory regime, it is inconsistent with the idea of case-by-case adjudication, which also puts paid to the idea that of a "common law of data security consent decrees":

> In this sense the FTC's data security settlements aren't an evolving common law — they are a static statement of "reasonable" practices, repeated about 55 times over the years and applied to a wide enough array of circumstances that it is reasonable to assume that they apply to *all* circumstances. This is consistency. But it isn't the common law. The common law requires consistency of application — a consistent theory of liability, which, given different circumstances, means *inconsistent* results. Instead, here we have consistent results which, given inconsistent facts, means [] *in*consistency of application.[207]

RECOMMENDATION: Allow Petitions for Appeal of Mooted Consent Decrees

Noticeably *not* addressed by this bill is the situation in which the FTC has found a company in violation of Section 5 for some practice (and imposed a consent decree for the violation), then lost in court on essentially the same doctrinal point. At a minimum, part of the reassessment of any consent decree should include assessing whether court decisions have called into question whether the original allegation actually violated Section 5. Ideally, the bill

---

[204] Fed. Trade Comm'n, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012) available at https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[205] *Id.*

[206] *See, e.g.*, *FTC's Google Settlement a Pyrrhic Victory for Privacy and the Rule of Law*, International Center for Law & Economics (Aug. 9, 2012), *available at* http://www.laweconcenter.org/component/content/article/84-ftcs-google-settlement-a-pyrrhic-victory-for-privacy-and-the-rule-of-law.html.

[207] Manne & Sperry, *supra* note 52, at 13.

should also include a procedure by which the company subject to a consent decree could petition for review of its consent decree on these grounds.

Such an amendment should not be controversial, given that the FTC so rarely (if ever) litigates its consumer protection cases.

Other Process Issues

Open Investigations

The Start Taking Action on Lingering Liabilities (STALL) Act

Rep. Susan Brooks' (R-IN) bill (H.R. 5097)[208] would automatically terminate investigations six months after the last communication from the FTC. Commission staff can keep an investigation alive either by sending a new communication to the target or the Commissioners can vote to keep the investigation open (without alerting the target). Current FTC rules allow the staff to inform targets that their investigation has ended, but does *not* require them to do so.[209]

VALUE OF THE BILL: Good Housekeeping, Reduces *In Terrorem* Effects of Lingering Investigations

This should be among the least controversial of the pending bills. It is simply a good housekeeping measure, ensuring that companies will not be left hanging in limbo after initial investigation-related communications from the FTC.

Closing open investigations could have several benefits.

First, in some circumstances, publicly traded companies may conclude that they are required to disclose the FTC's inquiry in their SEC filings.[210] That, in turn, can spark a media frenzy that could be as damaging to the company as whatever terms the FTC might impose in a consent decree — or at least seem to be less costly to managers who are more incentivized to care about the immediate performance of the company than the hassle of being sub-

---

[208] Start Taking Action on Lingering Liabilities Act, H.R. 5097, 114th Cong. (2016) [hereinafter STALL Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5097/text.

[209] Fed. Trade Comm'n, *Operating Manual: Chapter 3: Investigations*, 46 (last visited May 20, 2016), *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch03investigations_0.pdf (providing, in .3.7.4.5, that "[i]n investigations which have been approved by Bureau Directors, closing letters are ordinarily sent to both the applicant and the proposed respondent, with copies to their attorneys, if any[,]" but not requiring such letters in any case).

[210] *See, e.g.*, Deborah S. Birnbach, *Do You Have to Disclose a Government Investigation?*, *supra* note 99.

ject to an FTC consent decree for the next 20 years.[211] Making such disclosures can be particularly problematic if management intends to shop the company around for acquisition.

Presumably, a company that feels compelled to disclose an investigation in an SEC filling would, today, *eventually* feel justified in modifying the disclosure to indicate its belief that the investigation has concluded, given a long enough period of silence from the Commission. But this could take years, during which time the "lingering liability" could continue to damage the company. The bill (if it includes our proposed amendment, below) would give companies a clear indication whether or not they can modify their quarterly disclosures and inform shareholders and the general public that an investigation has concluded.

Second, giving subject companies repose after six months of silence from the FTC would allow management to focus on running their businesses. This could be especially critical for small companies.

Third, giving companies greater certainty in this way would reduce the leverage that staff may have to coerce companies into settling cases that might otherwise not be brought at all, or that companies might litigate. That means, in the first instance, moving closer to the optimal number of cases settled and, in the second instance, increasing the potential for litigation where it is warranted, which benefits everyone by allowing "the underlying criteria [of Section 5] to evolve and develop over time" through "judicial review," as the Unfairness Policy Statement explicitly intends.[212]

Fourth, holding target companies *in terrorem* may have other indirect costs besides driving companies to settle questionable cases. The longer an investigation lingers, or the longer it *could* linger (before the company can safely assume it is over), the more likely the company is to treat the FTC's "recommended" best practices as effectively mandatory, regulatory requirements. This regulation-by-terror is impossible to quantify, but it is a very real concern. To the extent it happens, it contributes to transforming the FTC's "inquisitorial powers" into a tool by which the FTC may treat its workshops and reports as de facto rulemakings, thus at least partially circumventing the Section 5 rulemaking safeguards.

Finally, the bill makes it harder for FTC staff to circumvent Bureau Director oversight — and thus avoid any possibility of alerting Commissioners. Current FTC rules allow an Initial Phase Investigation to be conducted for up to 100 hours of staff time, after which Staff must

---

[211] Notably, this also includes the potential for the FTC to bring additional enforcement actions premised on violating the terms of the consent decree, however attenuated the subsequent enforcement action might be, which is even easier than bringing an enforcement action premised directly on Section 5 (in that the FTC need not even purport to satisfy the requirements of Section 5). *See e.g.*, United States v. Google, Inc., Case 5:12-cv-04177-HRL (N.D.Ca. 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[212] UPS, *supra* note 9.

draft a memo and obtain approval from the Bureau Director to continue the investigation.[213] Today, the staff may be able to shoehorn a new investigation into an old investigation for which they have already received Director approval, thus avoiding or forestalling having to seek new approval from the Bureau Director. One can imagine that this would be particularly appealing if the Commission's majority — and thus also its Bureau Directors, who are appointed by the Chairman — has switched parties. This shoehorning may be very easy to do given the breadth of the FTC's investigations: one inquiry about questionable data security could very easily morph into another, potentially years later. The proposed bill would reduce this possibility by reducing the menu of available investigations from which staff could pick and choose. In other words, it would help to draw lines between old investigations and new ones. While this should not be a significant burden for the Staff, it should help to ensure that other internal decisionmaking safeguards are respected.

RECOMMENDATION: Bar Secret Votes as a Means of Evading the Bill

As drafted, the bill would allow the Commission to take a (non-public) vote to keep an investigation alive without the subject receiving additional communications. We can think of no reason to permit the Commission to hide the existence of a continuing investigation from its subject, however. In fact, although doing so requires a small price (an affirmative vote of the Commission), the price is so small that it is reasonable to expect that the exception would subsume the rule, and permit the Commission to evade the overall benefits of the proposed bill. Thus, we suggest amending section (2)(B) of the proposed bill, which authorizes an investigation to continue if "the Commission votes to extend the covered investigation before the expiration of such period,"[214] to also require the Commission to send a communication to the subject informing it of the vote. This would add no appreciable cost to the Commission's ability to extend an investigation, but, unlike a non-public vote, it ensures that the subject is made aware of the extension.

This amendment would have the benefit of allowing the subject's management to take *true* repose, knowing that an investigation had truly ended. Only then, for instance, would many managers feel comfortable revising a public securities disclosure about the company's lingering potential liability. In short, this would allow companies to clear their good names and get on with the business of serving consumers.

---

[213] Operating Manual at 9, § 3.2.1.1.

[214] STALL Act, *supra* note 208.

Commissioner Meetings

The Freeing Responsible & Effective Exchanges (FREE) Act

Rep. Pete Olson's (R-TX) bill (HR 5116)[215] would allow a bipartisan quorum of FTC Commissioners to meet confidentially under certain circumstances: no vote or agency action may be taken, the meeting must be FTC staff only, with a lawyer from the Office of General Counsel present, and the meeting must be disclosed publicly online. This would greatly empower other Commissioners by allowing them to meet with each other and with Commission staff — potentially without the Chairman, or without the Chairman having organized the meeting.

The bill does essentially the same thing as the FCC Process Reform Act of 2015 (H.R. 2583), which was so uncontroversial that it passed the House on a voice vote in November 2015.[216] Both bills would, for the affected agency, undo an unintended consequence of the Government in the Sunshine Act of 1976. That well-intentioned effort to bring transparency to agency decision-making in the aftermath of the Watergate scandal has the had the perverse result of undermining the very purpose of multi-member commissions.

VALUE OF THE BILL: Restoring the Collegiality of the FTC

The Sunshine Act calls multi-member commissions "collegial bod[ies],"[217] but the effect of the law has been to greatly contribute to the rise of the Imperial Chairmanship, because the law not only requires that "disposing of" (*i.e.*, voting on) major items (*e.g.*, rulemakings or enforcement actions) be conducted in public meetings (organized by the Chairman), it also bars Commissioners from "jointly conduct[ing]… agency business" except under the Act's tight rules. In effect, this makes it difficult for other Commissioners to coordinate without the Chairman.

The bill would continue to require that any "vote or any other agency action" be taken at meetings held under the Sunshine Act. This would ensure that the FTC generally continues to operate in full public view and according to valid process.

But the bill would allow Commissioners to meet privately, potentially without the Chairman present.

---

[215] The Freeing Responsible and Effective Exchanges Act, H.R. 5116, 114th Cong. (2016) [hereinafter FREE Act], *available at* https://www.congress.gov/bill/114th-congress/house-bill/5116/text.

[216] Federal Communications Commission Process Reform Act of 2015, H.R. 2583, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/2583/actions

[217] 5 U.S.C. § 552b(a)(1) & (3).

The benefits of such meetings are self-evident. They would encourage collegiality and facilitate bipartisan discussions, leading to a more open and inclusive process. They would also provide opportunities for minority commissioners to be apprised earlier in the process when the Commission is considering various actions, from investigations to issuing consent decrees.

The fact that the Energy & Commerce Committee has already vetted these reforms for the FCC, and that the full House has already voted for them as part of a larger FCC reform package, should make passage of this bill straightforward.

RECOMMENDATION: Ensure that Two of Three Commissioners Can Meet

As amended by the bill, 15 U.S.C. § 552b(d)(2)(A) would require that the group consist of at least three or more Commissioners. This would have the perverse result of rendering the bill useless at present, when the Commission has only three Commissioners — because all three would have to be present for a meeting. We recommend simply striking this subsection, so that, on a three-member commission, the Democrat and Republican commissioners can meet without the Chairman.

Part III Litigation

Numerous commentators have raised serious questions about the FTC's use of adjudication under Part III of the FTC's Rules. Commissioner Wright put it best in a 2015 speech:

> Perhaps the most obvious evidence of abuse of process is the fact that over the past two decades, the Commission has almost exclusively ruled in favor of FTC staff. That is, when the ALJ agrees with FTC staff in their role as Complaint Counsel, the Commission affirms liability essentially without fail; when the administrative law judge dares to disagree with FTC staff, the Commission almost universally reverses and finds liability. Justice Potter Stewart's observation that the only consistency in Section 7 of the Clayton Act in the 1960s was that "the Government always wins" applies with even greater force to modern FTC administrative adjudication.
>
> Occasionally, there are attempts to defend the FTC's perfect win rate in administrative adjudication by attributing the Commission's superior expertise at choosing winning cases. And don't get me wrong – I agree the agency is pretty good at picking cases. But **a 100% win rate is not pretty good; Michael Jordan was better than pretty good and made about 83.5% of his free throws during his career, and that was with nobody defending him. One hundred percent isn't Michael Jordan good; it is Michael Jordan in the cartoon movie "Space Jam" dunking from half-court good.** Besides being a facially implausible defense – the data also show appeals courts reverse Commission decisions at four times the rate of feder-

> al district court judges in antitrust cases suggests otherwise. This is difficult to square with the case-selection theory of the FTC's record in administrative adjudication.[218]

Former FTC Chairman Terry Calvani provides an apt summary of empirical research on the FTC's perfect win rate.[219] He notes FTC practitioner David Balto's study of eighteen years of FTC litigation, in which "the FTC has never found for the respondent and has reversed all ALJ decisions finding for the respondent."[220] Balto concluded "there appears to be a lack of impartiality by the Commission that really undermines the credibility of the process, and I think that makes it more difficult for the FTC to effectively litigate tough cases and get the court of appeals to support [its] decisions going forward."[221]

We recommend that Congress consider one of two structural reforms.

RECOMMENDATION: Separate the FTC's Enforcement & Adjudicatory Functions

Former Chairman Calvani proposes that

> the FTC be reorganized to separate the prosecutorial and adjudicatory functions. The former would be vested in a director of enforcement appointed by and serving at the pleasure of the president. Commissioners would hear the cases brought before the agency. This model is not alien to American administrative law and independent agencies. Labor complaints are evaluated and issued by National Labor Relations Board ("NLRB") regional directors. Administrative hearings are held before ALJs, and appeals from the ALJs are vested in the NLRB. Similarly, the Securities and Exchange Commission's ("SEC's") prosecutorial functions are vested in the Division of Enforcement while administrative hearings are held before ALJs and appeals are vested in the SEC.
>
> This change in organization would eliminate the existence or perception of unfairness associated with the same commissioners participating in both the decision to initiate a case and in its ultimate resolution. It would also make the deci-

---

[218] Joshua D. Wright, Commissioner, Fed. Trade Comm'n, *Remarks at the Global Antitrust Institute Invitational Moot Court Competition*,16-17 (Feb. 21, 2015) (emphasis added), *available at* https://www.ftc.gov/system/files/documents/public_statements/626231/150221judgingantitrust-1.pdf.

[219] Terry Calvani & Angela M. Diveley, *The FTC At 100: A Modest Proposal for Change*, 21 GEO. MASON L. REV. 1169, 1178-82 (2014).

[220] *Id.* at 1179 (quoting David A. Balto, *The FTC at a Crossroads: Can It Be Both Prosecutor and Judge?*, LEGAL BACKGROUNDER (Wash. Legal Found.) (Apr. 23, 2013), 1).

[221] Wash. Lgl Found., *FTC's Administrative Litigation Process: Should the Commission Be Both Prosecutor and Judge?*, YOUTUBE (Mar. 11, 2014), http://youtu.be/a9zvyDr4a-Y, at 9:24.

> sion to prosecute more transparent. One person would be responsible for the agency's enforcement agenda.[222]

Calvani notes that this would not significantly alter the responsibility of the powers of Commissioners, since "the power of a commissioner is relatively slight. The only real power of a commissioner is a negative one: blocking an enforcement initiative."[223] But it would "rather dramatically, [the responsibilities] of the chair."[224] In our view, this is a bug, not a feature.

RECOMMENDATION: Abolish or Limit Part III to Settlements

More fundamentally, Congress should re-examine the continued need for Part III as an alternative to litigation in Federal court. There are important differences between adjudications that originate in Part III proceedings as opposed to those that originate in Article III proceedings. Foremost, the selection of venue is an important determinant of the FTC's likelihood of success as well as the level of deference it will enjoy. Defendants will likewise see major differences between litigation in the different fora: from the range of discovery options available to the range and sort of materials considered by the tribunal (e.g., through amicus briefs). And, perhaps most important, the different venues each will create different legal norms and rules binding upon parties to future proceedings.

There is also a question regarding to what extent Part III proceedings are more than a mere formality. On the one hand, the FTC's Administrative Law Judge takes his job seriously, and has reversed the Commission in, most notably, two recent consumer protection decisions.[225] However, on the other hand, the Commission *always* reverses decisions of the ALJ that find against it.[226] Which leads to an important question: if the Commission is simply going to reverse its ALJ anyway what is the point of having an ALJ?

Even the threat of Part III litigation has a significant effect in coercing defendants to settle with the FTC during the investigation stage — not merely because of the direct financial costs of two additional rounds of litigation (first before the ALJ and then before the full Commission) prior to facing an independent Article III tribunal, but also because the Part III process drags out the other, less tangible but potentially far greater costs to the company in reputation and lost management attention. The threat of suffering two rounds of bad

---

[222] Calvani & Diveley, *supra* note 219, at 1184.

[223] *Id.* at 1185.

[224] *Id.* at 1184.

[225] In the Matter of LabMD, Inc., FTC File No. 102 3099 (May 16, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter; POM Wonderful LLC v. FTC, 777 F.3d 478 (D.C. Cir. 2015).

[226] Joshua D. Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, CPI ANTITRUST CHRONICLE, 4 (2012).

press before going to federal court (or at least one, if the ALJ rules for a defendant but the Commission reverses) may persuade some defendants who wouldn't otherwise to settle. Thus, the current operation of Part III rarely, if ever, serves to actually advance the interests of a fair hearing on disputed issues, and is more a tool to coerce settlements.

Congress could end this dynamic by requiring the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery. This is not a novel idea, nor would it be disruptive to the FTC as the Commission has had independent litigating authority since the 1970s.[227] The Smarter Act (H.R. 2745) effectively abolishes Part III with respect to merger cases, by requiring the FTC to bring Clayton Act Section 7 cases (for preliminary injunctions to stop mergers) in federal court under the same procedures as the Department of Justice.[228] This bill passed by a vote of 230 to 170.[229]

Finally, those who might object that abolishing Part III would hamstring the agency should take comfort in the fact that the FTC uses Part III so rarely anyway. Abolishing Part III will not bury the FTC in an avalanche of litigation in federal court. At most it would marginally increase the willingness of companies to resist the siren song of settlement, thus resulting in slightly more litigation (and perhaps also slightly more cases simply abandoned by staff, if they do not think they could win). But this is a trivial price to pay in comparison with the benefit of getting more judicial review and consistent enforcement standards and judicial standards of review. The difference between essentially no litigation and *some* litigation is the key difference between the Discretionary and Evolutionary Models.

RECOMMENDATION: Allow Commissioners to Limit the Use Part III

The least draconian reform would be to empower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective.

---

[227] Elliott Karr, *Essay: Independent Litigation Authority and Calls for the Views of the Solicitor General*, 77 GEO. WASH. L. REV. 1080, 1090-91 (2009).

[228] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/2745 [hereinafter SMARTER Act].

[229] U.S. House of Rep., *Final Vote Results For Roll Call 137* (Mar. 23, 2016) available at http://clerk.house.gov/evs/2016/roll137.xml

Standard for Settling Cases

No Bill Proposed

RECOMMENDATION: Set a Standard for Settling Cases Higher than for Bringing Complaints

Currently there is no standard for settling cases. The Commission simply applies the "reason to believe" standard set forth in Section 5(b) — and very often combines the vote as to whether to bring the complaint with the vote on whether to settle the matter, when the staff has already negotiated the settlement during the investigation process (because of the enormous leverage it has in this process, as we explain above). As Commissioner Wright has noted, "[w]hile the Act does not set forth a separate standard for accepting a consent decree, I believe that threshold should be at least as high as for bringing the initial complaint."[230] Reform in this area is especially critical if Congress chooses not to enact the "preponderance of the evidence" standard for issuing complaints.[231]

While it would certainly be an improvement to adopt even a "preponderance of the evidence" standard for the approval of consent decrees (relative to the status quo), we believe that this should be the standard for the approval of *complaints*, and that approval of *consent decrees* should be even higher (although, as we emphasis above, the "preponderance of the evidence" is not a particularly high standard).[232] The standard and process required by the Tunney Act for antitrust settlements would be a good place to begin. That act requires the FTC to file antitrust consent decrees with a federal court, and requires the court make the following determination:

> Before entering any consent judgment proposed by the United States under this section, the court shall determine that the entry of such judgment is in the public interest. For the purpose of such determination, the court shall consider:
>
> (A) the competitive impact of such judgment, including termination of alleged violations, provisions for enforcement and modification, duration of relief sought, anticipated effects of alternative remedies actually considered, whether its terms are ambiguous, and any other competitive considerations bearing upon the adequacy of such judgment that the court deems necessary to a determination of whether the consent judgment is in the public interest; and

---

[230] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Nomi Technologies, Inc., FTC. File No. 132 3251 (Sept. 3, 2015), 2, *available at* https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

[231] See, *supra*, at 18.

[232] *See infra* at 18.

> (B) the impact of entry of such judgment upon competition in the relevant market or markets, upon the public generally and individuals alleging specific injury from the violations set forth in the complaint including consideration of the public benefit, if any, to be derived from a determination of the issues at trial.[233]

If anything, a standard for settlements should require *more* analysis than this, as the Tunney Act has been relatively ineffective. In particular, any approach based on the Tunney act should allow third parties to intervene to challenge the FTC's assertions about the public interest.[234] This reform could go a long way toward inspiring the agency to perform more rigorous analysis.

Competition Advocacy

The FTC occupies a unique position in its role as the federal government's competition scold. Despite the absence of direct legal authority over federal, state and local actors (which limits the efficacy of competition advocacy efforts), some have argued that "the commitment of significant Commission resources to advocacy is nonetheless warranted by the past contributions of competition authorities to the reevaluation of regulatory barriers to rivalry, and by the magnitude and durability of anticompetitive effects caused by public restraints on competition."[235]

The FTC performs two different, but related, kinds of "competition advocacy":

1. **Competition advocacy *litigation***: The Bureau of Competition occasionally brings antitrust cases against nominally public bodies that the FTC believes are ineligible for state action immunity, either because they are effectively operating as marketplace participants (*e.g.*, state-run hospitals) or because state-created regulatory boards have been so completely coopted by private actors that they operate as private cartels, lacking sufficiently clear statement of legislative intent to maintain their state action immunity.
2. **Competition advocacy *filings***: The Office of Policy Planning files comments with state, local, tribal and federal lawmakers and regulators as to the impact of proposed (or existing) legislation or regulation upon consumers and competition.

---

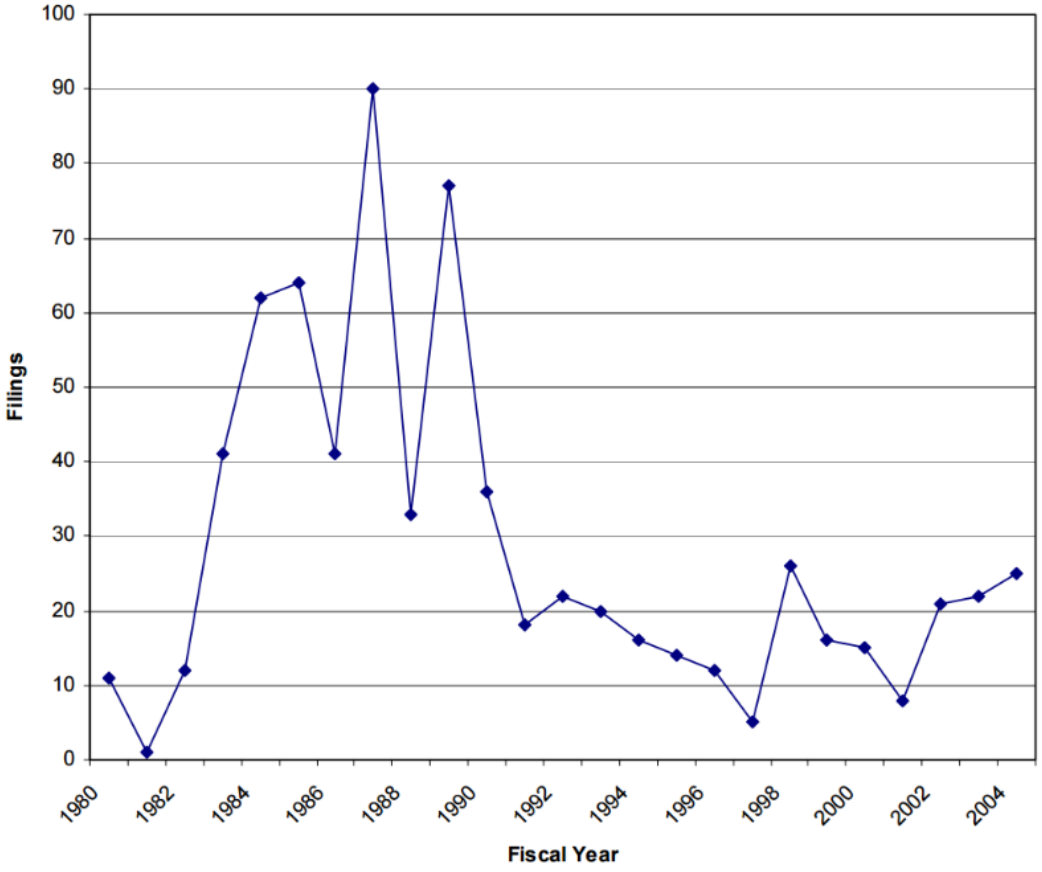
[233] 15 U.S.C. § 16(b)(1).

[234] The act currently provides that "Nothing in this section shall be construed to require the court to conduct an evidentiary hearing or to require the court to permit anyone to intervene." 15 U.S.C. § 16(b)(2).

[235] Ernest Gellhorn, & William E. Kovacic, *Analytical Approaches and Institutional Processes for Implementing Competition Policy Reforms by the Federal Trade Commission* (Dec. 12, 1995), *available at* https://www.ftc.gov/system/files/documents/public_statements/418071/951212comppolicy.pdf.

In 2004, James Cooper, Paul Pautler and Todd Zywicki (all FTC veterans) provided an empirical basis for comparing the FTC's level of activity on competition advocacy filings.[236] Their analysis included this chart:

FTC Advocacy Filings, 1980 to 2004[237]



Since 2009, the FTC has averaged just nineteen competition advocacy filings per year.[238] On high-tech matters, the Commission has been particularly inactive, making just four filings on ride-sharing,[239] four on direct sale of cars to consumers (*i.e.*, online),[240] and none on

---

[236] James C. Cooper, Paul A. Pautler & Todd J. Zywicki, *Theory and Practice of Competition Advocacy at the FTC* at 3, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/FTC%2090th%20Anniversary%20Symposium/040910zywicki.pdf.

[237] *Id.*

[238] A search of the FTC's Advocacy Filings reveals that between January 2009 and January 2016, 115 separate documents have been filed. *See* Fed Trade Comm'n, Advocacy Filings *available at* https://www.ftc.gov/policy/advocacy/advocacy-filings.

[239] Fed Trade Comm'n, "Transportation" Advocacy Filings, *available at* https://www.ftc.gov/policy/advocacy/advocacy-filngs?combine=&field_matter_number_value=&field_advocacy_document_terms_

(cont.)

house-sharing. It has also made few other broadly tech-related miscellaneous filings to other federal agencies on privacy and data security, vehicle-to-vehicle communications, mobile financial services, and the National Broadband Plan.

The FTC held a workshop on the sharing economy in June 2015,[241] but has since missed the opportunity to do significant competition advocacy work in the area, despite growing protectionist state and local regulation aimed at upstarts like Uber, Lyft, Airbnb and others. Recent legislation in Austin, Texas, is sadly illustrative. An Austin City Council ordinance,[242] essentially regulating ride-sharing services out of existence, was approved by (the few) voters who showed up to vote in a referendum.[243] This type of overly broad law regulating innovative technology is exactly the sort of thing the FTC should be taking initiative to advocate against, and it is unfortunate that, in the face of it, the FTC's competition advocacy has receded.

By contrast, in the early 2000s, OPP's State Action Task Force and Internet Task Force made a concerted effort to challenge anticompetitive state and local regulations that hindered online commerce through litigation, testimony and comments. The FTC started several campaigns, including one challenging rules making it harder to participate in e-commerce. Unlike the current Commission's stunted approach, the early 2000s FTC started with a workshop,[244] released reports explaining the problem the FTC's planned approach,[245]

---

tid=5283&field_date_value%5Bmin%5D%5Bdate%5D=January%2C+2009&field_date_value%5Bmax%5D%5Bdate%5D=January%2C+2016&items_per_page=100.

[240] Fed Trade Comm'n, "Automobiles" Advocacy Filings, *available at* https://goo.gl/lq9ACP.

[241] Fed. Trade Comm'n, The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators (Jun. 9, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators

[242] Austin, Texas, Ordinance No. 20151217-075 (2015), *available at* http://www.austintexas.gov/edims/document.cfm%3Fid=245769.

[243] Jared Meyer, *The Reverse of Progress. Austin's new rules strangle Uber, Lyft – and the ridesharing economy,* U.S. NEWS & WORLD REPORT (May 18, 2016), *available at* http://www.usnews.com/opinion/articles/2016-05-18/austins-very-un-progressive-example-on-uber-and-lyft.

[244] Fed. Trade Comm'n Workshop, Possible Anticompetitive Efforts to Restrict Competition on the Internet, Oct. 8-10, 2002, *available at* https://www.ftc.gov/news-events/events-calendar/2002/10/possible-anticompetitive-efforts-restrict-competition-internet.

[245] FED. TRADE COMM'N, REPORT OF THE STATE ACTION TASK FORCE (2003), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/report-state-action-task-force/stateactionreport.pdf; FED. TRADE COMM'N, POSSIBLE ANTICOMPETITIVE BARRIERS TO E-COMMERCE: WINE (2003), *available* at https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-report-concerning-possible-anticompetitive-barriers-e-commerce-wine/winereport2.pdf; FED. TRADE COMM'N, POSSIBLE BARRIERS TO E-COMMERCE: CONTACT LENSES: A REPORT FROM THE STAFF OF THE FEDERAL TRADE COMMISSION (Mar. 29, 2004), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/possible-anticompetitive-barriers-e-commerce-contact-lenses-report-staff-ftc/040329clreportfinal.pdf.

and then went on to systematically challenge e-commerce-related regulations (among other things) inconsistent with consumer welfare. Filings included:

- Comment on Ohio legislation to allow direct shipment of wine to Ohio consumers;[246] and on similar New York legislation;[247]
- Congressional Testimony regarding online wine sales;[248]
- Comment on Arkansas legislation regarding online contact sales;[249] and
- Comment on Connecticut regulation of contact sales.[250]

The current FTC has many ripe targets for public interest advocacy around the nation as incumbents are, predictably, using regulation to try to stop Internet- and app-based competition, especially disruptive new "sharing economy" business models.

VALUE OF THE IDEA: Competition Advocacy Is the Most Cost-Effective Way to Serve Consumers

As Cooper, Pautler & Zywicki explain:

> The economic theory of regulation ("ETR") posits that because of relatively high organizational and transaction costs, consumers will be disadvantaged relative to businesses in securing favorable regulation. This situation tends to result in regulations — such as unauthorized practice of law rules or per se prohibitions on sales-below-cost — that protect certain industries from competition at the expense of consumers. Competition advocacy helps solve consumers' collective ac-

---

[246] Comment on Proposed Direct Shipment Legislation of the Federal Trade Commission to the Ohio State Senate (2006), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-eric-d.fingerhut-concerning-ohio-s.b.179-allow-direct-shipment-wine-ohio-consumers/v060010commentreohiosb179directshipmentofwine.pdf

[247] *Letter of the Federal Trade Commission regarding Assembly bill 9560-A, Senate bills 6060-A and 1192 to the New York State legislature (2004)*, https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-william-magee-et-al.concerning-new-york.b.9560-s.b.606-and-s.b.1192-allow-out-state-vendors-ship-wine-directly-new-york-consumers/v040012.pdf

[248] Prepared Statement of Todd Zywicki, Fed. Trade Comm'n, before the Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce United States House of Representatives (Oct. 13, 2003), available at https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-statement-u.s.house-representatives-energy-and-commerce-concerning-e-commerce-wine-sales-and-direct-shipment/031030ecommercewine.pdf

[249] *Letter of the Federal Trade Commission regarding Arkansas HB 2286 to the Arkansas House of Representatives (2015)*, *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-honorable-doug-matayo-concerning-arkansas-h.b.2286-and-fairness-contact-lens-consumers-act-and-contact-lens-rule/041008matayocomment.pdf.

[250] Comments of the Staff Of the Federal Trade Commission In Re: Declaratory Ruling Proceeding on the Interpretation and Applicability of Various Statutes and Regulations Concerning the Sale of Contact Lenses (2002), *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-connecticut-board-examiners-opticians-intervenor-re-declaratory-ruling-proceeding/v020007.pdf

> tion problem by acting within the political system to advocate for regulations that do not restrict competition unless there is a compelling consumer protection rationale for imposing such costs on citizens. Furthermore, advocacy can be the most efficient means to pursue the FTC's mission, and when antitrust immunities are likely to render the FTC impotent to wage ex post challenges to anticompetitive conduct, advocacy may be the only tool to carry out the FTC's mission.[251]

Competition advocacy is probably the most cost-effective way the FTC can promote consumer welfare. Anticompetitive practices and agreements backed up by the power of the state are much less likely to be corrected by the power of competition than those that exist in the marketplace, and antitrust law cannot be used to remove such barriers to competition. The only way for the FTC to even get at such conduct is through its competition advocacy arm.

RECOMMENDATION: Clarify Section 6(f) & the FTC May File Unsolicited Comments

The FTC currently relies on Sections 6(a) (information gathering) and 6(f) (issuance of reports) as the basis for its competition advocacy filings.[252] But as discussed above,[253] Section 6(f) could be read to allow the FTC to make recommendations for legislation only to Congress, not to states or local governments. This is the kind of small discontinuity between the statute's plain meaning and the agency's practice (on an issue that enjoys broad bipartisan support) that should be addressed by Congress in regular reauthorization.

In the same vein, we gather that, if only by standing convention, the FTC does not file comments with state and local lawmakers or regulators unless invited to do so by someone on the relevant body. This is undoubtedly well-intentioned, perhaps grounded in some kind of sense of federalism, but it may have the perverse result of denying consumers the benefit of the FTC's competition-advocacy work where it is most needed: when state regulators are so captured by incumbents, or otherwise blinded to the benefits of new technologies, that they will resent the FTC's comment as an intrusion upon their decision-making.

We urge Congress to kill two birds with one stone by amending Section 6(f) to add the following bolded text (and, for clarity's sake, roman numeral subsection numbers):

---

[251] Cooper, Pautler & Zywicki, *Theory and Practice of Competition Advocacy at the FTC supra* note 236, at 2.

[252] See, e.g., *id.* at 1, n.3:

> The legal authority for competition advocacy is found in Section 6 of the FTC Act, which allows the FTC to "gather and compile information" that concerns persons subject to the FTC Act, and "to make public such portions of the information obtained" that are "in the public interest."

(Quoting 15 U.S.C. § 46(a), (f) (2005)).

[253] *See supra* 61.

> To (i) make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to (ii) make annual and special reports to the Congress and to submit therewith recommendations for additional legislation; ***and to (iii) file recommendations for legislation or regulatory action with state, local, tribal and federal bodies***; and to (iv) provide for the publication of its reports and decisions in such form and manner as may be best adapted for public information and use

RECOMMENDATION: Create an Office of Bureau of Competition Advocacy with Dedicated Funding

The FTC's Competition advocacy *filing* function has languished, in part, because while competition advocacy *litigation* resides inside the Bureau of Competition, the filings are primarily the responsibility of the Office of Policy Planning (OPP), a relatively tiny organization attached to the Chairman's office, which has a staff of just over a dozen compared to 285 for the Bureau of Competition, 331 for the Bureau of Consumer Protection, and 114 for the Bureau of Economics.[254]

Congress should seriously consider creating an independent office of Competition Advocacy, which would manage competition-advocacy filings, and share joint responsibility for competition-advocacy litigation with the Bureau of Competition. In particular, this would mean giving this new Bureau a line item in the FTC's budget.

RECOMMENDATION: In the Alternative, Reconstitute the Task Force

As noted above, the Internet Task Force, which was spun off from the broader State Action Task Force, had considerable effect through its research, reports, and associated filings. A standing Task Force of this nature could provide dividends by picking up where the Sharing Economy Workshop left off and studying the effects of regulation on the sharing economy around the nation. A well-done report could then be followed by strategic litigation, amicus briefs, and other filings in order to promote sound public policy and combat the Internet-age protectionism that is slowing down innovation and competition and the attendant benefit to consumers.

Expanding FTC Jurisdiction

Section 5 of the FTC Act empowers the Commission to prevent unfair and deceptive acts and practices by nearly all American businesses (and business people). The exceptions are

---

[254] *Cf.* Fed. Trade Comm'n, Federal Trade Commission Office of Policy Planning Organizational Chart, https://www.ftc.gov/system/files/attachments/office-policy-planning/opp-org-chart-may2016.pdf; Fed. Trade Comm'n, Shutdown of Federal Trade Commission Operations Upon Failure of the Congress to Enact Appropriations, https://www.ftc.gov/system/files/attachments/office-executive-director/130925ftcshutdownplan.pdf.

few: "banks, savings and loan institutions…, federal credit unions…, common carriers subject to the Acts to regulate commerce, air carriers and [certain meat packers and stockyards]...." One important limitation is that the FTC Act does not expressly give the Commission jurisdiction over nonprofit organizations. Nevertheless, courts have held that nonprofit status is not in itself sufficient to exempt an organization from FTC jurisdiction.[255] In *Cal Dental Ass'n v. FTC*, the Supreme Court noted that the FTC has jurisdiction over both "'an entity organized to carry on business for its own profit' … [as well as] one that carries on business for the profit 'of its members.'"[256] Thus, various types of nonprofits — notably trade associations — can be reached by the FTC *depending on their activities*, but "purely charitable" organizations remain outside of the FTC's enforcement purview.[257]

Subcommittee Democrats have revived two sensible proposals from 2008 to expand the FTC's jurisdiction. Both have long enjoyed bipartisan support, and have been endorsed by the Commission under both Republican and Democratic chairmen.

FTC Jurisdiction over Common Carriers

The Protecting Consumers in Commerce Act of 2016

Jerry McNerney's (D-CA) bill (H.R. 5239)[258] would allow the FTC to regulate common carriers currently regulated by the Federal Communications Commission. In particular, this would ensure that the FTC and FCC have dual jurisdiction over broadband — effectively restoring the jurisdiction the FTC lost when the FCC "reclassified" broadband in 2015.

The FCC recently issued a controversial NPRM proposing privacy and data security rules for broadband that are significantly different from the approach the FTC has taken. This bill would moot the need for new FCC privacy and data security rules as a "gap filler." The bill would also allow the FTC to police net neutrality concerns, interconnection and other broadband practices (to the extent it finds unfair or deceptive practices) even if the FCC's Open Internet Order fails in pending litigation.

---

[255] *See, e.g.*, Community Blood Bank v. FTC, 405 F.2d 1011 (8th Cir. 1969).

[256] Cal. Dental Ass'n v. FTC, 526 U.S. 756, 766 (1999).

[257] *See Statement of William C. Macleod, Dir. of FTC Bureau of Consumer Protection, Before The U.S. House of Representatives Committee on Energy & Commerce; Subcommittee on Transportation & Hazardous Materials; Hearing On Deceptive Fundraising By Charities* (Jul. 28, 1989), *available at* http://www.freespeechcoalition.org/macleod.htm.

[258] Protecting Consumers in Commerce Act of 2016, H.R. 5239, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/5239/text.

VALUE OF THE BILL: Reclassification of Broadband by the FCC Should Not Remove FTC Jurisdiction

There has long been unusual bipartisan agreement on ending the common carrier exemption. This was proposed by Sen. Byron Dorgan's proposed FTC Reauthorization Act of 2002,[259] and supported by Republican Commissioner Thomas Leary and Democrat Commissioner Sheila Anthony.[260] Sen. Dorgan last proposed the same reform in 2008.[261] More recently, in 2015, Democrat Chairman Edith Ramirez and Republican Commissioner Josh Wright supported this reform.[262]

Section 5 jurisdiction excludes "common carriers subject to the Acts to regulate commerce."[263] The bill simply edits the definition of "Acts to regulate commerce" in Section 4 to remove the Communications Act.[264] Thus, the FTC *could* regulate common carriers regulated by the FCC but *not* transportation common carriers.

Former Commissioner Joshua Wright summarized the many advantages of keeping the FTC as a cop on the broadband beat:

> The FTC has certain enforcement tools at its disposal that are not available to the FCC. Unlike the FCC, the FTC can bring enforcement cases in federal district court and can obtain equitable remedies such as consumer redress. The FCC has only administrative proceedings at its disposal, and rather than obtain court-ordered consumer redress, the FCC can require only a "forfeiture" payment. In addition, the FTC is not bound by a one-year statute of limitations as is the FCC. The FTC's ability to proceed in federal district court to obtain equitable remedies that fully redress consumers for the entirety of their injuries provides comprehen-

---

[259] Federal Trade Commission Reauthorization Act of 2002, S. 2946, 104th Cong. (2002), *available at* https://www.congress.gov/bill/107th-congress/senate-bill/2946/text.

[260] *Additional Statement of Commissioner Thomas B. Leary*, *Hearing Before the H. Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2003), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-reauthorization/030611learyhr.pdf; Federal Trade Commission Testifies Before Senate in Support of Reauthorization Request for Fiscal Years 2003 to 2005, *available at* https://www.ftc.gov/es/node/63553.

[261] Federal Trade Commission Reauthorization Act of 2008, S. 2831 §14, 110th Cong. (2008), *available at* https://www.govtrack.us/congress/bills/110/s2831/text

[262] *Prepared Statement of Commissioner Joshua D. Wright, Federal Trade Commission: Wrecking the Internet to Save It? The FCC's Net Neutrality Rule Before the H. Comm. on the Judiciary*. 114th Cong. (2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/632771/150325wreckinginternet.pdf; Ramirez urges repeal of common carrier exemption, FTC WATCH, *available at* http://www.ftcwatch.com/ramirez-urges-repeal-of-common-carrier-exemption/.

[263] 15 U.S.C. § 45(a)(2).

[264] *Cf.* 15 U.S.C. § 44.

sive consumer protection and can play an important role in deterring consumer protection violations.[265]

RECOMMENDATION: Pass the Protecting Consumers in Commerce Act to End the Exemption for Telecom Common Carriers

Ending the common carrier exemption for telecom companies is long overdue. "As the telecommunications and Internet industries continue to converge, the common carrier exemption is likely to frustrate the FTC's efforts to combat unfair or deceptive acts and practices and unfair methods of competition in these interconnected markets."[266] Moreover, the uncertainty surrounding the application of the exemption to new technologies, as well as the long-standing uncertainty around application of the exemption to non-common-carrier activities carried out by common carriers introduce needless administrative costs.

RECOMMENDATION: Require the FCC to Terminate Its Privacy Rulemaking

With respect to the common carrier exception, the fortunes of the FTC are tied to those of the FCC; adopting optimal policy for one requires adopting complimentary policy for the other. The conclusions above are complicated by the FCC's ongoing efforts to exercise the *exclusive* authority it claimed when it reclassified Internet service providers as common carriers, particularly with respect to privacy and similar matters.[267] Because the FCC's rationale for its proposed privacy rules is to fill the gap it created by "reclassifying" broadband and thus removing it from the FTC's jurisdiction, enactment of this legislation would moot the need for new FCC rules. Accordingly, this bill should include a provision directing the FCC to terminate that rulemaking — so that the FTC may resume its former role in policing broadband privacy and data security without unnecessary and costly duplicative regulations.

This situation is very much unlike that in the 1980 FTC Improvements Act, by which Congress both tightened the FTC's Section 5 rulemaking processes (as instituted in 1975) and also ended the FTC's children's advertising rulemaking.[268] In signing the bill, President Carter lauded the former but objected to the latter:

---

[265] *Prepared Statement of Commissioner Joshua D. Wright*, *supra, available at* https://www.ftc.gov/system/files/documents/public_statements/632771/150325wreckinginternet.pdf (internal citations omitted).

[266] FED TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION REPORT, 41 (2007), *available at* https://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf.

[267] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, WC Docket No. 16-106 (rel. Apr. 1, 2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

[268] FTC Improvements Act Section 11 added the following language to 17 U.S.C. § 57a: "The Commission shall not have any authority to promulgate any rule in the children's advertising proceeding pending on the date of the enactment of the Federal Trade Commission Improvements Ante, p. 374. Act of 1980 or in any

(cont.)

> We need vigorous congressional oversight of regulatory agencies. But the reauthorization bills passed by the Senate and the House went beyond such oversight and actually required termination of specific, major, ongoing proceedings before the Commission. I am pleased that the conferees have modified these provisions. If powerful interests can turn to the political arena as an alternative to the legal process, our system of justice will not function in a fair and orderly fashion.[269]

President Carter had a point, in general. But in this case, Congress would not be telling an agency to stop a pending rulemaking because of a policy difference; it would be telling the FCC to stop a rulemaking that it claims is necessary only because of a regulatory vacuum of its own creation.

If the FCC insists on issuing its own rules, the bill will result in overlapping jurisdiction, which could create problems of its own: forum-shopping, inconsistent results, and politicization of the enforcement process. The Memorandum of Understanding reached between the two agencies on how to handle enforcement where their authority *does* overlap will do little to minimize potential conflicts.[270] It would be particularly incongruous to enact legislation authorizing overlapping and conflicting jurisdiction while Congress is also considering the SMARTER Act, aimed at mitigating exactly such problematic overlap in the antitrust enforcement authority of the FTC and DOJ.[271] None of these concerns are inherent reasons not to restore the FTC's jurisdiction; after all, the FTC is the better regulator, in large part because applying standards of general applicability makes the FTC a more difficult agency to capture than a sector-specific regulator like the FCC. But these concerns do make it important that passage of this bill be tied to ending the FCC's foray into privacy and data-security regulation.

FTC Jurisdiction over Tax-Exempt Organizations & Nonprofits

The Tax Exempt Organizations Act

Representative Rush's (D-IL) bill (H.R. 5255)[272] would add tax-exempt, 501(c)(3) nonprofits to the definition of "corporation" subject to the FTC Act in Section 4 (15 U.S.C. § 44). It

---

substantially similar proceeding on the basis of a determination by the Commission that such advertising constitutes an unfair act or practice in or affecting commerce."

[269] Carter, *supra* note 19.

[270] Memorandum of Understanding on Consumer Protection Between the Federal Trade Commission and the Federal Communications Commission (Nov. 2015), *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

[271] SMARTER Act, *supra* note 228.

[272] A Bill to Amend the Federal Trade Commission Act to Permit the Federal Trade Commission to Enforce Such Act Against Certain Tax-exempt Organizations, H.R. 5255, 114th Cong. (2016) *available at* https://www.congress.gov/bill/114th-congress/house-bill/5255/text.

would not, however, amend Section 4 to remove the language that limits the FTC's jurisdiction to corporations that "carry on business for [their] own profit or that of [their] members." Thus, the FTC would still be limited to policing for-profit activities but would have an easier time establishing that a nonprofit was essentially conducting for-profit activities.

VALUE OF THE BILL: Would Reduce Litigation Expenses for the FTC

This bill does precisely the same thing proposed by Sen. Byron Dorgan's FTC Reauthorization Act of 2008.[273] The Republican-led FTC supported this provision at the time.[274]

In 2008, in supporting Sen. Dorgan's version of this bill, the FTC explained the advantage of this reform, even though it would not technically change the substance of the FTC's jurisdiction:

> The proposed legislation would also help increase certainty and reduce litigation costs in this area. Although the FTC has been successful in asserting jurisdiction against "sham" nonprofits and against non-profit trade associations, the proposed legislation would help avoid protracted factual inquiries and litigation battles to establish jurisdiction over such entities.[275]

We agree with the FTC's 2008 assessment.

RECOMMENDATION: Extend Jurisdiction to Tax-Exempt Entities, Including Trade Associations

In 2008, in supporting Sen. Dorgan's version of this bill, the FTC also said:

> The Commission would be pleased to work with Congressional staff on crafting appropriate language. The Commission notes that, as drafted, Section 6 would reach only those non-profit entities that have tax-exempt status under section 501(c)(3) of the Internal Revenue Code. The Commission would benefit from broadening this provision to cover certain other nonprofits, such as Section 501(c)(6) trade associations. The Commission has previously engaged in protracted litigation battles to determine whether such entities are currently covered under the FTC Act. *See, e.g., California Dental Ass'n v. FTC*, 526 U.S. 756, 765-69 (1999) (holding that FTC Act applies to anticompetitive conduct by non-profit dental association whose activities provide substantial economic benefits to for-profit members); *American Medical Ass'n v. FTC*, 638 F.2d 443, 447-448 (1980) (finding FTC jurisdiction over non-profit medical societies whose activities

---

[273] Federal Trade Commission Reauthorization Act of 2008, *supra* note *261*, § 6, *available at* https://www.govtrack.us/congress/bills/110/s2831/text.

[274] *Prepared Statement of the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Science, and Transportation*. 110th Cong. (2008), 19, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/ftc-testimony-reauthorization/p034101reauth.pdf.

[275] *Id*. at 16.

"serve both the business and non-business interests of their member physicians").[276]

RECOMMENDATION: Extend Jurisdiction to *All* Non-Profits

We likewise recommend expanding the bill to encompass all nonprofit corporations, regardless of their tax-exempt status.[277] The logic of the FTC's jurisdiction doesn't turn on the tax-exempt status of organizations, which, for these purposes, is essentially a meaningless dividing line between entities. It makes little sense to include tax-exempt nonprofits within the FTC's ambit while excluding nonprofits without federal tax-exempt status.

Rulemaking

The FTC makes rules in two ways: (1) under Section 5, through the process created by Congress in 1980 to require additional economic rigor and evidence; and (2) under narrow grants of standard APA rulemaking authority specific to a particular issue.

Economic Analysis in All FTC Rulemakings

No Bill Proposed

RECOMMENDATION: Require BE to Comment on Rulemakings

The RECS Act, discussed below, would require the FTC to include BE analysis of any recommendations it makes for rulemakings. However, this would not apply to the FTC's own rulemakings because that bill is focused on the FTC's statutory authority to make recommendations to Congress, other agencies, and state and local governments.

Requiring regulatory agencies to do cost-benefit analysis has been uncontroversial for decades, dating back at least to the Carter Administration. Indeed, in 2011, shortly after President Obama issued Executive Order 13563,[278] his version of President Clinton's 1993 Executive Order 12866[279] applying to Executive Branch agencies, he issued a second order, Regu-

---

[276] *Id.* at 18 n.49.

[277] The nonprofit designation is a creature of state incorporation law, and obligates corporations to adopt certain governance rules and structures. Federal tax-exempt status is a creature of federal tax law, and, while it obligates companies to limit their corporate purpose (*e.g.*, to education, religious activities, etc.), it doesn't appreciably affect their governance structure. Companies can be nonprofit but not tax-exempt, although all tax-exempt companies are nonprofit.

[278] Exec. Order No. 13,563, 3 C.F.R. 13563 (2012) *available at* https://www.whitehouse.gov/the-press-office/2011/01/18/executive-order-13563-improving-regulation-and-regulatory-review.

[279] Exec. Order No. 12,866 3 C.F.R. 12866 (1993) *available at* https://www.whitehouse.gov/sites/default/files/omb/inforeg/eo12866/eo12866_10041993.pdf.

lation and Independent Regulatory Agencies, Executive Order 13579.[280] The key difference between the two is that the President said Executive agencies "must" do cost-benefit analysis for each new regulation, but that independent agencies "should" undertake retrospective analysis of its rules and periodically update them.

FTC Chairman Jon Leibowitz fully endorsed the idea in the White House's blog about the Order:

> President Obama deserves enormous credit for ensuring regulatory review throughout the federal government, including at independent agencies. Although regulations are critically important for protecting consumers, they need to be reviewed on a regular basis to ensure that they are up-to-date, effective, and not overly burdensome. For all agencies – independent or not – periodic reviews of your rules is just good government. The announcement raises the profile of this issue, and I think that's a constructive step.[281]

The chief (indeed, perhaps the only) reason for the difference is that the President has no authority over independent agencies, which are creatures and servants of Congress. The bipartisan Independent Agency Regulatory Analysis Act of 2015 (S. 1607) would solve this problem, giving the President the authority to set cost-benefit standards for independent agencies as well.[282] We fully support that bill and believe this requirement should apply to *all* independent agencies. But there is no reason to wait for passage of the more comprehensive bill. The FTC in particular would benefit from a commitment to cost-benefit analysis in its rulemakings immediately.

Of course, it is true that the Commission has abandoned using its Section 5 rulemaking power (precisely because it reflects the Carter-era commitment to cost-benefit analysis). But the Commission *does* continue to make rules under a variety of issue-specific statutes such as several of those now pending before the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade in May 2016.[283] As the chief example of the need for greater economic rigor in FTC rulemakings, we note the FTC's 2012 COPPA rulemaking: the agency expanded the definition of "personal information," thus greatly

---

[280] Exec. Order No. 13,579, 3 C.F.R. 13579 (2012) *available at* https://www.whitehouse.gov/the-press-office/2011/07/11/executive-order-13579-regulation-and-independent-regulatory-agencies.

[281] Cass Sunstein, *The President's Executive Order on Improving and Streamlining Regulation by Independent Regulatory Agencies*, WHITEHOUSE.GOV BLOG (Jul. 11, 2011), https://www.whitehouse.gov/blog/2011/07/11/president-s-executive-order-improving-and-streamlining-regulation-independent-regula.

[282] Independent Agency Regulatory Analysis Act of 2015, S. 1607, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/1607/text.

[283] *See* Press Release, HEARING: #SubCMT to Review 17 Bills Modernizing the FTC for the 21st Century NEXT WEEK, THE ENERGY AND COMMERCE COMMITTEE (May 17, 2016), https://energycommerce.house.gov/news-center/press-releases/hearing-subcmt-review-17-bills-modernizing-ftc-21st-century-next-week.

expanding the number of children's-oriented media subject to the rule, with no meaningful analysis of what this would do to children's media.

Despite loud protests from small operators that the rule might cause them to cease offering child-oriented products, the FTC produced a meaningless estimate that the rule would cost $21.5 million in the aggregate.[284] Of course, the *real* cost of the new rule is not the direct compliance cost but the second-order effects of the number of providers who exit the children's' market, reduce functionality, slow innovation or raise prices — none of which did the FTC even attempt to estimate. This was a clear failure of economic analysis.

We also note Commissioner Ohlhausen's 2015 dissent from the Commission's vote to update the Telemarketing Sales Rule to ban telemarketers from using four "novel" payment methods. Ohlhausen cited no less an authority than the Federal Reserve Bank of Atlanta (FRBA), which is not merely one of twelve Federal Reserve Branches, but the one responsible for "operat[ing] the Federal Reserve System's Retail Payments Product Office, which manages and oversees the check and Automated Clearing House (ACH) services that the Federal Reserve banks provide to U.S. financial institutions."[285] Ohlhausen explained:

> The amendments do not satisfy the third prong of the unfairness analysis in Section 5(n) of the FTC Act, which requires us to balance consumer injury against countervailing benefits to consumers or competition. Although the record shows there is consumer injury from the use of novel payment methods in telemarketing fraud, it is not clear that this injury likely outweighs the countervailing benefits to consumers and competition of permitting novel payments methods….
>
> In sum, the FRBA's analysis of the prohibition of novel payments in telemarketing indicates that any reduction in consumer harm from telemarketing fraud is outweighed by the likely benefits to consumers and competition of avoiding a fragmented law of payments, not limiting the use of novel payments prematurely, and allowing financial regulators working with industry to develop better consumer protections.[286]

Again, it appears that the Commission majority failed to undertake an economically rigorous analysis of the sort BE would likely perform, in this case failing to properly weigh injury and countervailing benefits as Section 5(n) requires.

---

[284] 78 Fed. Reg. 4002 *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

[285] Separate Statement of Commissioner Maureen K. Ohlhausen, Dissenting in Part, In the Matter of the Telemarketing Sales Rule, Project No. R411001, at n. 3 (Nov. 18, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/881203/151118tsrmkospeech.pdf.

[286] *Id.* at 1-2.

At a minimum, the Commission would have done well to solicit further public comment on its rule, heeding the experience of past chairmen, as summarized by Former Chairman Tim Muris:

> By their nature, however, rules also must apply to legitimate actors, who actually deliver the goods and services they promise. Remedies and approaches that are entirely appropriate for bad actors can be extremely burdensome when applied to legitimate businesses, and there is usually no easy or straightforward way to limit a rule to fraud. Rather than enhancing consumer welfare, overly burdensome rules can harm the very market processes that serve consumers' interests. For example, the Commission's initial proposal for the Telemarketing Sales Rule was extremely broad and burdensome, and one of the first acts of the Pitofsky Commission was to narrow the rule. More recently, the Commission found it necessary to re-propose its Business Opportunity Rule, because the initial proposal would have adversely affected millions of self-employed workers.[287]

Issue-Specific Rulemakings

Several Bills Proposed

Congress has long enacted legislation tasking the FTC with enacting regulations in a specific area through standard rulemaking under the Administrative Procedure Act. This, in effect, has allowed the FTC to avoid having to conduct rulemakings under the Magnuson-Moss Act of 1975 (as amended in 1980). The result has been that there may not be anyone left at the FTC who has ever conducted a Section 5 rulemaking. This contributes to the common misconception that the FTC lacks rulemaking authority — something the Chairman and other Commissioners have said casually. Of course, they mean that the FTC lacks *APA* rulemaking authority, and that they believe Section 5 rulemaking is too difficult.

But this belief is unfounded. There is good reason to think that the FTC could have conducted a Section 5 rulemaking to address telemarketing complaints, for example, in about the same amount of time it took Congress to pass the Do Not Call Act and for the FTC to conduct an APA rulemaking, and perhaps even less. As Former Chairman Tim Muris explained, in 2010:

> The Commission's most prominent rulemaking endeavor, the creation of the National Do Not Call Registry, could have proceeded in a timely fashion under Magnuson-Moss procedures. It took two years from the time the rule was first publicly discussed until it was implemented. Although it would have been neces-

[287] *Statement of Timothy J. Muris, supra* note 14, at 24.

> sary to structure the proceedings differently, there would have been little, if any, additional delay from using Magnuson-Moss procedures.[288]

This is not idle speculation. Muris actually ran the FTC during its creation of the Do Not Call registry. Attempting a Section 5 rulemaking would have been a valuable experience for the FTC, and it might have avoided some of the unintended consequences of ex ante legislation.

We make two broad recommendations applicable to all six rulemaking bills.

RECOMMENDATION: Require the FTC to Conduct Section 5 Rulemakings & Report on the Process

The FTC would greatly benefit from conducting a Section 5 rulemaking. Congress should direct the FTC to conduct such a rulemaking on at least one, and preferably two or three, of the issues to be addressed by these proposed issue-specific bills. Having multiple rulemakings would produce a more representative experience with the FTC's Section 5 rulemaking powers. However many Section 5 rulemakings the FTC does, Congress should direct the FTC to report back in, say, three years as to the state of these rulemakings and the FTC's general experience with its Section 5 rulemaking procedures. This is the only way Congress will ever be able to make informed decisions about how existing Section 5 rulemaking processes might be expedited or streamlined without removing the safeguards that Congress rightly imposed to prevent the FTC from abusing its rulemaking powers.

Any reconsideration of the FTC's Section 5 rulemaking processes should be undertaken with the utmost caution. Unfairness is a uniquely elastic concept, which requires unique procedural safeguards if it is to serve as the basis for rulemaking. If anything, FTC's approach to enforcing Section 5 in high tech matters over the last 15–20 years reconfirms the need for safeguards: in its "common law of consent decrees," the FTC has paid little more than lip service to the balancing test inherent in unfairness, and has increasingly nullified the materiality requirement at the heart of the deception policy statement.

RECOMMENDATION: Include Periodic Re-Assessment Requirements in Any New Grants of APA Rulemaking Authority

It is impossible to predict the unintended consequences of any of the proposed issue-specific bills granting the FTC new rulemaking authority.[289] However narrowly targeted they may

---

[288] *Id.* at 27.

[289] *See* Press Release, *#SubCMT Releases Reform Package to Modernize the FTC and Promote Innovation*, THE ENERGY AND COMMERCE COMMITTEE (May 5, 2016), https://energycommerce.house.gov/news-center/press-releases/subcmt-releases-reform-package-modernize-ftc-and-promote-innovation.

seem, they may wind up constraining new technologies or business models that would otherwise serve consumers.

Consider the Video Privacy Protection Act of 1988 ("VPPA"), which barred "wrongful disclosure of video tape rental or sale records."[290] After the experience of Judge Robert Bork, whose video rental records were made an issue at his (failed) Supreme Court confirmation hearings, this quick-fix bill must have seemed utterly uncontroversial. Yet it proved overly rigid in the digital age. In 2009, an anonymous plaintiff sued Netflix over its release of data sets for the Netflix Prize, alleging that the company's release of the information constituted a violation of the VPPA.[291] In 2011 Netflix launched a feature integrating its service with Facebook — everywhere *except* in the U.S., citing the 2009 lawsuit and concerns over the VPPA. After two years, President Obama signed legislation (H.R. 6671) amending the VPPA to allow Netflix and other video companies to *give consumers the option* of sharing information about their viewing history on social networking sites like Facebook.[292] Despite this amendment, the VPPA continues to threaten to overly restrict novel online transactions that were never contemplated or intended by the drafters of the statute.[293]

The VPPA is just one of many laws that have proven unable to keep up with technological change (the 1996 Telecommunications Act, (largely) a classic example of the Rulemaking Model, comes readily to mind). To protect against this inevitability, Congress should include regular review of legislation as a "safety hatch." The 1998 Children's Online Privacy Protection Act (COPPA) included this review provision:

> Not later than 5 years after the effective date of the regulations initially issued under … this title, the Commission shall —
>
> (1) review the implementation of this chapter, including the effect of the implementation of this chapter on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and (2) prepare and submit to Congress a report on the results of the review under paragraph (1).[294]

---

[290] Video Privacy Protection Act of 1988, Pub. L. 100-618, 102 Stat. 3195 (Nov. 5, 1988), *available at* https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf.

[291] *See* Kristian Stout, *Pushing Ad Networks Out of Business: Yershov v. Gannett and the War Against Online Platforms*, TRUTH ON THE MARKET (May 10, 2016), https://truthonthemarket.com/2016/05/10/pushing-ad-networks-out-of-business-yershov-v-gannett-and-the-war-against-online-platforms/.

[292] Video Privacy Protection Act Amendments Act of 2012, H.R. 6671, 112th Cong (2012), *available at* https://www.congress.gov/bill/112th-congress/house-bill/6671?q=%7B%22search%22%3A%5B%22%5C%22hr6671%5C%22%22%5D%7D&resultIndex=1.

[293] *See* Stout, *supra* note 291.

[294] 15 U.S.C. § 6506.

In principle, this is the right idea. However, in practice, this requirement has proven ineffective. The FTC's review of COPPA included little meaningful analysis of the cost of COPPA.[295] Indeed, the FTC used the discretion afforded it by Congress in the statute to expand the definition of the term "personal information" in ways that appear to have reduced the availability, affordability and diversity of children's media — yet without any economic analysis by the Commission.

At a minimum, Congress should include something like the following in any issue-specific grant of new APA rulemaking authority it enacts:

> Not later than 5 years after the effective date of the regulations initially issued under… this title, ***and every 5 years thereafter,*** the Commission shall —
>
> (1) ***direct the Bureau of Economics, with the assistance of the Office of Technology Research and Investigation,*** to review the implementation of this chapter, including the effect of the implementation of this chapter on practices relating to ***[affected industries]***; and
>
> (2) prepare and submit to Congress a report on the results of the review under paragraph (1).

Conclusion

The letter by which the FTC submitted the Unfairness Policy Statement to the Chairman and Ranking Member of the Senate Commerce Committee in December 1980 concludes as follows:

> We hope this letter has given you the information that you require. Please do not hesitate to call if we can be of any further assistance. With best regards,
>
> /s/Michael Pertschuk, Chairman[296]

We believe it's high time Congress picked up the phone.

To be effective, any effort to reform the FTC would require a constructive dialogue with the Commission — not just those currently sitting on the Commission, but past Commissioners and the agency's staff, including veterans of the agency. Along with the community of practitioners who navigate the agency on behalf of companies and civil society alike, all of these will have something to add. We do not presume to fully understand the inner workings of the Commission as only veterans of the agency can. Nor do we presume that the ideas presented here are necessarily the best or only ones to accomplish the task at hand. But reform

---

[295] *See supra* note 284.

[296] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

cannot be effective if it begins from the presumption that today's is the "best of all possible FTCs," or that any significant reform to the agency would cripple it.

Unfortunately, many of those who would tend to know the most about the inner workings of the agency are also the most blinded by status quo bias, the tendency not just to take for granted that the FTC works, and has always worked, well, but to dismiss proposals for change as an attacks upon the agency. It would be ironic, indeed, if an agency that wields its own discretion so freely in the name of flexibility and adaptation were itself unwilling to adapt.

We believe that reforms to push the FTC back towards the Evolutionary Model can be part of a bipartisan overhaul and reauthorization of the agency, just as they were in 1980 and 1994. At stake is much more than how the FTC operates; it is nothing less than the authority of Congress as the body of our democratically elected representatives to steer the FTC. Congress should not, as Justice Scalia warned in 2014 in *UARG v. EPA*, willingly "stand on the dock and wave goodbye as [the FTC] embarks on this multiyear voyage of discovery."[297]

[297] Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2446 (2014).

No. 16-16270

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

LabMD, Inc.,

***Petitioner*,**

v.

Federal Trade Commission,

***Respondent*.**

On Petition for Review from the Federal Trade Commission, *In the Matter of LabMD, Inc.*, FTC Matter/File Number: 102 3099, Docket Number: 9357

AMICUS CURIAE BRIEF OF INTERNATIONAL CENTER FOR LAW & ECONOMICS AND TECHFREEDOM IN SUPPORT OF PETITIONER, LABMD, INC.

Geoffrey A. Manne
Kristian Stout
INTERNATIONAL CENTER
FOR LAW & ECONOMICS
3333 NE Sandy Blvd., Suite 207
Portland, OR 97232
503-770-0076
gmanne@laweconcenter.org

Berin M. Szóka
Thomas W. Struble
TECHFREEDOM
110 Maryland Avenue, Suite 409
Washington, DC 20002
202-803-2867
bszoka@techfreedom.org

John P. Hutchins*
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

* *Counsel of Record*

UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

LABMD, INC, Petitioner, v. FEDERAL TRADE COMMISSION, Respondent.	)	Case File No. 16-16270 FTC Docket No. 9357

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT (CIP)

Pursuant to Fed. R. App. P. 26.1 and 11th Cir. R. 26.1-1(a), International Center for Law & Economics and TechFreedom, by and through their undersigned counsel, hereby state that neither entity has a parent corporation and that no publicly held corporation owns ten percent or more of either entity's stock. A listing of all known trial judges, attorneys, persons, associations of persons, firms, partnerships, or corporations that have an interest in the outcome of this case or appeal, including subsidiaries, conglomerates, affiliates, parent corporations, any publicly held corporation that owns 10% or more of the party's stock, and other identifiable legal entities related to a party follows:

Barrickman, Allred & Young, LLC, Counsel for Scott Moulton

Bavasi, Haley, Attorney, Ropes & Gray LLP

Berger, Laura, Attorney, FTC

Boback, Robert J., nonparty below

Brill, Julie, Former Commissioner, FTC

Brown, Jarad A., Attorney, FTC

Brown, Reginald J., Attorney, Counsel for Tiversa

Bryan Cave LLP, Counsel for Richard Wallace

Buchanan, Mary Beth, Attorney, Bryan Cave LLP

Burrows, Robyn N., Attorney, formerly of Cause of Action

Cause of Action, Counsel for LabMD

Chappell, D. Michael, Chief Administrative Law Judge, FTC

Clark, Donald S., Secretary, FTC

Claybaugh, Melinda, Attorney, FTC

Cohen, David T., Attorney, Ropes & Gray LLP

Cox, Megan, Attorney, FTC

Daugherty, Michael J., Chief Executive Officer, LabMD

Dinsmore & Shohl LLP, Counsel for LabMD

Epstein, Daniel Z., Attorney, formerly of Cause of Action

Federal Trade Commission ("FTC"), Respondent

Feldman, John P., Attorney, Reed Smith LLP

Forensic Strategy Services, LLC, nonparty below

Gelsomini, Nicole, Attorney, Ropes & Gray LLP

Gersh, Deborah L., Attorney, Ropes & Gray LLP

Hallward-Driemeier, Douglas, Attorney, Ropes & Gray LLP

Harris, Lorinda B., Attorney, formerly of Cause of Action

Harris, Sunni R., Attorney, Dinsmore & Shohl LLP

Hoffman, Matthew M., Attorney, FTC

Howard, Elizabeth G., Attorney, Barrickman, Allred & Young, LLC

Huntington, Kent G., Attorney, formerly of Cause of Action

International Center for Law & Economics

Johnson, M. Eric, Professor, Vanderbilt University

Kaufman, Daniel, Deputy Director, FTC Bureau of Consumer Protection

Khetan, Prashant K., Attorney, formerly of Cause of Action

Kotlyar, Leon, Attorney, Ropes & Gray LLP

Krebs, John, Attorney, FTC

LabMD, Inc., Petitioner

Lassack, Margaret L., Attorney, FTC

Lattimore, Ashton R., Attorney, Ropes & Gray LLP

Lechner, Jr., Alfred J., Attorney, Cause of Action

Manne, Geoffrey A., Attorney, International Center for Law & Economics

Marcus, Joel, Attorney, FTC

Marshall, Erica L., Attorney, Cause of Action

Massari, Patrick J., Attorney, Cause of Action

McSweeny, Terrell, Commissioner, FTC

Meal, Douglas H., Attorney, Ropes & Gray LLP

Mehm, Ryan M., Attorney, FTC

Metzler, Jr., Theodore P., Attorney, FTC

Morgan, Hallee K., Attorney, Cause of Action

Moulton, Scott, President, Forensic Strategy Services, LLC, nonparty below

Moundas, Christine, Attorney, Ropes & Gray LLP

Nordsieck, David W., Attorney, Ropes & Gray LLP

Ohlhausen, Maureen K., Commissioner, FTC

O'Leary, Kevin D., Associate General Counsel, Dartmouth College

Pepson, Michael D., Attorney, Cause of Action

Ramirez, Edith, Chairwoman, FTC

Reed Smith LLP, Counsel for Robert J. Boback and Tiversa

Ropes & Gray LLP, Counsel for LabMD

Rubinstein, Reed D., Attorney, Dinsmore & Shohl LLP

Santiesteban, Joseph, Attorney, Ropes & Gray LLP

Schell, Jacquelyn N., Attorney, Bryan Cave LLP

Schoshinski, Robert, Assistant Director, FTC

Settlemyer, Carl H., Attorney, FTC

Shaw, Jarrod D., Attorney, Reed Smith LLP

Sheer, Alain, Attorney, FTC

Sherman, II, William A., Attorney, Dinsmore & Shohl LLP

Shonka, David C., Attorney, FTC

Stout, Kristian, Attorney, International Center for Law & Economics

Struble, Thomas, Attorney, TechFreedom

Szoka, Berin, Attorney, TechFreedom

TechFreedom, amicus curiae below

Tiversa Holding Corporation, nonparty below

Tiversa, Inc., nonparty below

VanDruff, Laura Riposo, Attorney, FTC

Visser, Michelle L., Attorney, Ropes & Gray LLP

Wallace, Richard, nonparty below

Wright, Joshua D., Former Commissioner, FTC

Yodaiken, Ruth, Attorney, FTC

No publicly traded company or corporation has an interest in the outcome of the case or appeal.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

LABMD, INC, Petitioner, v. FEDERAL TRADE COMMISSION, Respondent.	)	Case File No. 16-16270 FTC Docket No. 9357

STATEMENT OF AUTHORSHIP & FINANCIAL CONTRIBUTIONS

Under Federal Rule of Appellate Procedure 29(c), *amici* state that no party's counsel authored this brief in whole or in part, and no party or its counsel made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae or their counsel contributed money that was intended to fund preparing or submitting the brief.

STATEMENT OF INTEREST

ICLE is a non-profit, non-partisan global research and policy center. ICLE works with more than fifty affiliated scholars and research centers around the world to promote the use of evidence-based methodologies in de-

veloping sensible, economically grounded policies that will enable businesses and innovation to flourish.

TechFreedom is a non-profit, non-partisan 501(c)(3) tax-exempt think tank dedicated to educating policymakers, the media and the public about technology policy. TechFreedom advocates regulatory approaches that balance the need for flexibility with analytical rigor to constrain regulatory discretion.

TechFreedom and ICLE have convened the FTC: Technology & Reform Project, dedicated to studying the details of the agency's operations and proposing reforms to help the agency achieve its mission of maximizing consumer welfare. *See, e.g.*, CONSUMER PROTECTION & COMPETITION REGULATION IN A HIGH-TECH WORLD: DISCUSSING THE FUTURE OF THE FEDERAL TRADE COMMISSION (Dec. 2013), *available at* http://goo.gl/52G4nL.

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Other Authorities

Rules

SUMMARY OF THE ARGUMENT

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ["Section 5"], is a consumer protection statute, not a data security rule. *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, United States Senate (Dec. 17, 1980) ["Unfairness Statement"], reprinted in *International Harvester Co.*, 104 FTC 949, 1073 (1984) ["*International Harvester*"]

(quoting 83 Cong. Rec. 3255 (1938) (remarks of Senator Wheeler)) ("Unjustified consumer injury is the primary focus of the FTC Act….'").

This fundamental point has been lost in the Commission's approach to data security. The touchstone for Section 5 actions is not "reasonableness," but consumer welfare: Does this enforcement action deter a preventable "unfair" act or practice that, on net, harms consumer welfare, and do the benefits to consumers from this action outweigh its costs? Section 5's purpose is neither fundamentally remedial nor prescriptive. Concern for consumer welfare means deterring bad conduct, avoiding over-deterrence of pro-consumer conduct, minimizing compliance costs, and minimizing administrative costs (by focusing only on substantial harms) — *not* preventing every possible harm. Instead of weighing such factors carefully, or even performing a proper analysis of negligence, as it purports to do, the Commission has effectively created a strict liability standard unmoored from Section 5.

Across the Commission's purported guidance on data security, it has likewise failed to articulate a standard by which companies themselves should weigh costs and benefits to determine which risks are sufficiently foreseeable that they can be mitigated cost-effectively. Thus, in addition to violating the intent of Congress, the FTC has also violated the Constitution by failing to

provide companies like LabMD with "fair notice" of the agency's interpretation of what Section 5 requires.

For the following reasons, the FTC's Order should be vacated.

ARGUMENT

I. THE FTC PROVIDED INSUFFICIENT NOTICE OF THE DATA SECURITY REQUIREMENTS UNDER SECTION 5 OF THE FTC ACT TO COMPORT WITH DUE PROCESS.

The FTC alleges that, between June 2007 and May 2008, LabMD violated Section 5 of the FTC Act by failing to provide "reasonable" data security. *In re LabMD, Inc.*, Administrative Complaint, F.T.C. Docket No. 9357 (Aug. 29, 2013) ["Complaint"]. Contrary to the view of the FTC, but in keeping with that of its Chief Administrative Law Judge, *In re LabMD, Inc.*, Initial Decision, F.T.C. Docket No. 9357 (Nov. 13, 2015) ["Initial Decision"], the FTC failed to provide, *during this period*, the fair notice required by the Constitution to LabMD that its data security could be deemed unfair. As a plainly exasperated district court judge said to FTC's counsel during a hearing on the FTC's denial of LabMD's motion to dismiss:

> I think that you will admit that there are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…. [H]ow does any company in the United States operate when… [it] says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are

> not supposed to do what you did.… [Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.

Transcript of Proceedings at 91, 94–95, *LabMD, Inc. v. Fed. Trade Comm'n*, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014) ["Oral Argument Transcript"]. Thus, lacking such notice, the FTC's Order finding LabMD's data security violated Section 5 of the Act was in violation of LabMD's due process rights, and should be vacated. *In re LabMD, Inc.*, Final Order, F.T.C. Docket No. 9357 (July 29, 2016) ["Order"].

A. **The FTC Misreads the Case Law on Fair Notice**

The FTC relies heavily upon *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 (3d Cir. 2015) ["*Wyndham*"], but fundamentally misunderstands the case. The FTC claims that the agency has

> provided ample notice to the public of our expectations regarding reasonable and appropriate data security practices by issuing numerous administrative decisions finding specific companies liable for unreasonable data security practices. Our complaints, as well as our decisions and orders accepting consent decrees…make clear that the failure to take reasonable data security measures may constitute an unfair practice. Those complaints, decisions, and orders also flesh out the specific types of security lapses that may be deemed unreasonable.… And even though they "are neither regulations nor 'adjudications on the merits,'" they are sufficient to afford fair notice of what was needed to satisfy Section 5(n). *See Wyndham*, 799 F.3d at 257 (citing *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004) ["*Lachman*"]; *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008) ["*Beverly*"];

> and *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) ["*General Electric*"]).

In re LabMD, Inc., Opinion of the Commission, F.T.C. Docket No. 9357, at 30–31 (July 29, 2016) ["FTC Opinion"]. This misreads *Wyndham*: as an interlocutory appeal from the denial of a 12(b)(6) motion, the decision did not determine whether the FTC's informal data security guidance had provided fair notice. *Wyndham*, 799 F.3d at 240.

The Third Circuit merely noted that "courts regularly *consider* materials that are neither regulations nor 'adjudications on the merits.'" *Id.* at 257 (emphasis added). Whether such agency guidance affords fair notice depends on the circumstances. *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MAS. L. REV. 673, 704–05 (2013).

Crucially, the sufficiency of such materials to confer fair notice in each of the three cases cited by *Wyndham* (and relied upon by the FTC) turns on the reasonableness of expecting the defendant to create an adequate internal compliance regime based on (i) monitoring the agency's interpretations and pronouncements, and (ii) effectively predicting how the agency would apply its authority. Each analysis also hinged on the company's experience as a special-

ly regulated enterprise vis-à-vis a particular agency — in a way that is not true of LabMD and the FTC:

- *Lachman*: Manufacturer of "carbon/carbon material…suitable for use in rocket components, including ballistic missiles with nuclear capability" could not claim it lacked fair notice that its product would require an export license; it had a duty to consult counsel regarding how the Commerce Department would apply the term "specially designed" to its product. 387 F.3d at 45, 57.

- *Beverly*: Nursing home had fair notice of an advice letter issued by OSHA fifteen years earlier declaring that employers of healthcare professionals must reimburse employees exposed to blood-borne pathogens not only for direct medical costs, but also for travel costs, and compensation for time spent recovering. 541 F.3d. at 202.

- *General Electric*: Manufacturer of large electric transformers lacked fair notice of the EPA's interpretation of its regulation on disposing of a dangerous chemical because the agency's "policy statements [were] unclear…the [company's] interpretation [was] rea-

> sonable, and … the agency itself struggle[d] to provide a definitive reading of the regulatory requirements." 53 F.3d at 1334.

All three cases involved regulations "addressed to sophisticated businessmen and corporations which, because of the complexity of the regulatory regime, necessarily consult counsel in planning their activities." *Lachman*, 387 F.3d at 57.

The FTC effectively imputes this burden to any company in America that holds personal data. But the FTC differs fundamentally from the Commerce Department enforcing export control regulations or the EPA policing toxic substances — or even HHS regulating the data practices of healthcare companies. The FTC is America's catch-all consumer protection regulator; it polices nearly every company in America under the most general possible standards. This case is readily distinguishable from *Beverly*: yes, the FTC and OSHA both enjoy broad jurisdiction ("trade" and "workplaces") but OSHA enforced a statute explicitly focused on the topic at issue (*i.e.*, "wage loss" and "medical expenses"), 29 U.S.C. § 651(a). The only question was the precise application of those terms, a question that OSHA answered with a clear statement including the very issues in dispute (time spent receiving treatment and travel expenses). *Beverly*, 541 F.3d. at 197. The FTC, by contrast, is enforcing a vague statutory standard (unfairness) with a vague regulatory standard (unrea-

sonableness) and offering guidance whose applicability is unclear — and is not the regulator assigned by Congress to the issue.

The implication from this line of cases is clear: entities, like LabMD, comprehensively regulated under industry-specific regimes, have a duty to be aware of the requirements of those specialized regimes. But, to the extent that other federal regulatory regimes purport to impose *differing* requirements on those companies, fair notice of those different requirements cannot be presumed. This is particularly true where the specialized regulatory regime enforces detailed regulations relating to the issue under consideration.

The FTC occasionally brings actions against HHS-regulated companies and has sporadically opined on health-related data security issues, *see, e.g.*, *In the Matter of CVS/Caremark Corp.*, Dkt. No. C-4259, FTC File No. 0723119 (2009), http://bit.ly/2hMjDNH (2009); *In the Matter of Rite-Aid Corp.*, Dkt. No. C-4308, FTC File No. 0723121 (2010), http://bit.ly/2hMcU6z; Medical Identity Theft Guidance: FAQ'S for Health Care Providers and Health Plans, FTC (2011), *available at* https://goo.gl/6S61SH. But not only does this not suffice to establish the FTC as a sectoral regulator commanding the close attention of industry actors, the first of these actions and guidance documents long postdated the conduct at issue here.

Meanwhile, HHS energetically enforces its own data security rules, and yet, during the time period relevant here, never offered guidance directing its covered entities or business associates to look to the FTC, nor referred to FTC guidance or enforcement actions relating to data security and privacy. *See* "Security," hhs.gov (last visited Jan. 2, 2017), http://bit.ly/2hJhDWC (referring only to FTC guidelines promulgated in 2010 and later, and not referring to enforcement at all). In fact, HHS and FTC have often been at loggerheads over data enforcement.[1]

The Supreme Court has repeatedly that, where they diverge, specialized, comprehensive regulatory regimes supersede more generalized regimes that address overlapping issues. See, e.g., *Credit Suisse Securities v. Billing*, 551 U.S. 264 (2007); *Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398 (2004); *United States v. Citizens Southern Nat. Bank*, 422 U.S. 86 (1975).

B. The FTC Misreads *Wyndham* More Generally.

The FTC generally misreads the *Wyndham* opinion. The Third Circuit repeatedly expressed skepticism of the FTC's notice arguments. Most funda-

[1] Not until October 2016 did the FTC and HHS declare that covered entities and business associates should look to both agencies for guidance regarding certain PHI practices. *See* "Sharing Consumer Health Information? Look to HIPAA and the FTC Act," FTC and HHS, *available at* http://bit.ly/2hJfKcw.

mentally, the court dismissed the relevance of the FTC's enforcement actions and focused instead on the statute itself. *Wyndham*, 799 F.3d at 255–59.

The relevant question is not merely whether LabMD had fair notice that Section 5 might apply to data security, *id.* at 255 ("We do not read Wyndham's briefs as arguing [it] lacked fair notice that cybersecurity practices can … form the basis of an unfair practice"), but whether LabMD had fair notice as to *how* the FTC would apply the cost-benefit analysis test in Section 5 to its data security. *Id.* ("Wyndham argues instead that it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability.") (emphasis in original). This is the difference, between saying that General Electric had a special duty to monitor to the EPA's pronouncements and that General Electric had fair notice of *how* the EPA would interpret a particular rule. *See Gen. Elec. Co.*, 53 F.3d at 1334.

On that question, the *Wyndham* court implied strongly that the FTC's guidance was insufficient to qualify as fair notice. *See Wyndham*, 799 F.3d at 256 n.21 ("we agree with Wyndham that the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question."); *id.* at 257 n.22 ("We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective

requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).").

C. The FTC's *Guidance* Did Not Provide LabMD *Fair* Notice, and the Order Thus Violates Due Process.

The FTC points to various guidance it had produced contemporaneous with the LabMD data theft. But such guidance was insufficient to afford LabMD fair notice.

The FTC's first document on the topic, *Protecting Personal Information: A Guide For Business*, FTC (2007), *available at* https://goo.gl/w9fSfW, issued in March 2007 — very shortly before the LabMD data theft — suggested at least some of the data security practices the FTC alleges LabMD should have provided. Previously, the FTC had issued only one press release (2004) and workshop report (2005, geared towards developers of peer-to-peer networking software) to point to for guidance. FTC Opinion, at 30 n.81 (citing Press Release, Press Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure (Apr. 2, 2004), and *Protecting Personal Information*, FTC (2005)). And the FTC also cited evidence of common industry practice, but that evidence was from 2010, a full two years *after* the relevant time period. But, given the timing of its guide, the size and sophistication of LabMD, and

the nature of the allegedly unreasonable behavior, the FTC's guidance did not provide *fair* notice.

In claiming that its press releases and workshop reports qualify as sufficient guidance to provide fair notice, the FTC is treating these highly informal statements as triggers of legally enforceable duties — *i.e.*, *de facto* rulemakings. For example, the FTC routinely cites its 2012 Privacy Report, Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) ["FTC Privacy Report"], *available at* http://bit.ly/2hMz7RX, as if it were a rulemaking, incorporating its "recommendations" as boilerplate, welding them onto every data security settlement, regardless of the circumstances. *See, e.g.*, Gus Hurwitz, *FTC's Efforts in* LabMD *Lack Required Due Process and Don't Actually Improve Security*, TECHPOLICYDAILY.COM (Aug. 2, 2016), http://bit.ly/2hNZtTu.

Thus has the Commission circumvented the rulemaking safeguards established by Congress in the Magnuson-Moss Act of 1975, 15 U.S.C. § 57b-3, and tightened by Congress in 1980, Federal Trade Commission Improvements Act of 1980, Pub. L. 96-252, 94 Stat. 374 (1980) — the same Congress that forced the FTC to issue the Unfairness Statement. Whatever discretion administrative agencies enjoy in choosing to use either rulemakings or case-by-case

adjudication, the FTC's attempt to shoehorn these quasi-regulatory soft guidance materials into fair notice raises profound due process concerns.

II. THE FTC'S "REASONABLENESS" STANDARD EXCEEDS ITS AUTHORITY UNDER SECTION 5

Consumer welfare is the lodestar of Section 5. Like the consumer welfare-oriented antitrust laws, Section 5 does not proscribe specific acts but is a general standard, designed to penalize and deter "unfair" conduct that harms consumers on net – *without* sweeping in pro-consumer conduct that does not cause demonstrable harm (or that is "reasonably avoidable" by consumers themselves). *See* FTC Opinion at 26 (quoting Unfairness Statement, at 1073) ("A 'benefit' can be in the form of lower costs and… lower prices for consumers, and the Commission 'will not find that a practice unfairly injures consumers unless it is injurious in its net effects.'").

Thus, Section 5(n) incorporates a negligence-like standard, rather than a strict-liability rule, and thus concepts from the common law, such as foreseeability and duty of care. Thus, the FTC may prohibit only conduct whose costs outweigh benefits, and where harm isn't more efficiently avoided by consumers themselves. *See, e.g.*, Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (Jun. 5, 2001), *available at* https://goo.gl/0LPP5w (emphasizing these ele-

ments of the FTC's unfairness inquiry and finding no responsibility for unforeseeable risks).

Establishing that conduct was unfair/unreasonable thus requires establishing (i) a clear baseline of conduct, (ii) a company's deviation from that baseline, and (iii) proof that its deviation caused, or was significantly likely to cause, harm. Both the statute and the constitutional doctrine of Fair Notice require *some* limits on the FTC's discretion to decide what, beyond the existence of a breach, indicates inadequate data security.

The FTC's rhetoric on data security appears to reflect the fundamental negligence-like analysis and economic balancing required by Section 5(n):

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities…. [T]he Commission… does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

Commission Statement Marking the FTC's 50th Data Security Settlement at 1 (Jan. 31, 2014) ["FTC 50th Settlement Statement"], *available at* http://bit.ly/2hubiwv*; see also* FTC Opinion at 11. Yet, by eliding the distinct elements of a Section 5(n) analysis, the FTC's "reasonableness" approach ends

up ignoring Congress's plain requirement that the Commission demonstrate causality and substantiality, and perform a cost-benefit analysis — clearly rejecting a strict liability approach. Congress plainly intended to constrain the FTC's discretion to avoid the hasty assumption that imposing *any* costs on consumers is "unfair."[2]

The FTC claims it has weighed the relevant facts, but has failed to adduce how specific facts affect its analysis, demonstrate causation, or evaluate the relative costs and benefits of challenged practices and its own remedies. The Commission asserts that the exposed data were sensitive, but said nothing, for example, about (i) whether any of it (*e.g.*, medical test codes) could actually reveal sensitive information; (ii) what proportion of LabMD's sensitive data was exposed on LimeWire; (iii) the complexity or size of the business; (iv) the indirect costs of compliance, such as the opportunity costs of implementation of the FTC's required remedies; and (v) the deterrent effect of the enforcement action.

The FTC's inappropriately *post hoc* assessment considers only those remedial measures it claims would address the specific breach at issue. This ignores the overall compliance burden to avoid liability without knowing, *ex*

[2] No market interaction is *ever* without costs: paying any price, waiting in line, or putting up with advertising are all "costs" to a consumer.

ante, which specific harm might occur. Actual compliance costs are far more substantial, and require a firm to evaluate which of the universe of possible harms it should avoid, and which standards the FTC has and would enforce. This is a far more substantial, costlier undertaking than the FTC admits.

A. The FTC Failed to Establish that LabMD Breached Its Duty of Care

Section 5(n) plainly requires a demonstrable connection between conduct and injury. While the anticompetitive harm requirement that now defines Sherman Act jurisprudence was a judicial construct, *see, e.g., Continental T.V., Inc. v. GTE Sylvania, Inc.*, 433 U.S. 36 (1977), Section 5(n) itself demands proof that an "act or practice causes or is likely to cause substantial injury" before it may be declared unfair. But the FTC's reasonableness approach, as noted, is not directed by the statute, which nowhere defines actionable conduct as "unreasonable;" rather, the statute requires considerably more. But even taking the FTC at face value and assuming "reasonableness" is meant as shorthand for the full range of elements required by Section 5(n), the FTC's approach to reasonableness is fatally wanting.

1. The FTC Has Not Established a Benchmark Standard for Duty of Care

Although reasonableness is a fuzzy concept, courts have developed consistent criteria for establishing it. Under negligence standards, an actor must

have, and breach, a duty of care before its conduct will be deemed unreasonable. *See* STUART M. SPEISER ET AL., 2A AMERICAN LAW OF TORTS, § 9:3 (2016). This requires that the actor's duty be defined with enough specificity to make it clear when her conduct breaches it — which is not true here, reasons that parallel why LabMD lacked fair notice of how the FTC would apply Section 5 to it.

In most jurisdictions, "care" is defined by reference to standard industry practices, specific legislative requirements, contractual obligations, or a judicial determination of what prudence dictates. Restatement (Second) of Torts § 285 (1965). Moreover, in most jurisdictions, the appropriate standard of care reflects the foreseeability of harm: there is no duty to protect against unforeseeable risks. *Id.* § 302.

The FTC has established no concrete benchmark for due care, however. The Commission cites in passing to some possible sources, *see, e.g.,* FTC Opinion at 12 (referring to HIPAA as "a useful benchmark for reasonable behavior"), but fails to distinguish among such documents, to explain how much weight to give any of them, or to distill these references into an operationalizable standard. Not only was this true at the time of LabMD's alleged conduct, but it remained the case six to seven years *later*, and arguably still holds true today:

> the standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as "*un*reasonable" — and, by negation, reasonable — privacy and data security procedures.

Patricia Bailin, *What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, IAPP/Westin Research Center Study, at 1 (Oct. 30, 2014), *available at* http://bit.ly/2hJkIWR.

Moreover, because of the amorphousness of the FTC's data security "standards", and the fact that they are developed through one-sided consent decrees with limited application and little, if any, legal analysis,

> *we don't know what we don't know*, that is, whether other practices that have not yet been addressed by the FTC are "reasonable" or not. (In fact, we don't even know whether there is … a comprehensive FTC data security standard). Even in those cases that have been pursued, we don't know how high the reasonableness bar is set. Would it be enough for a company to elevate its game by just an increment to clear the reasonableness standard? Or does it have to climb several steps to clear the bar?

Omer Tene, *The Blind Men, the Elephant and the FTC's Data Security Standards*, PRIVACY PERSPECTIVES BLOG (Oct. 20, 2014), *available at* http://bit.ly/2hJwlwI (emphasis in original). Again, this was only *more* true at the time of LabMD's conduct, when the FTC's unfairness approach to data security was in its infancy.

Not only does this defect cause the action against LabMD to fail for lack of fair notice, as discussed above, it also causes the action to exceed the Commission's statutory authority.

2. The FTC Failed to Establish that LabMD's Conduct Deviated from its Duty of Care

Because "perfect" data security is impossible, not all data security practices that "increase" risk of breach are unfair. *See* FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement", (Jan. 31, 2014) ("the Commission has made clear that it does not require perfect security"). *Some* amount of harm (to say nothing of breaches) is fully consistent with the exercise of due care — of "reasonable" data security practices. For the statute to be meaningful, data security practices must be shown to fall outside of customary practice — *i.e.*, to increase the risk of unauthorized exposure (and the resulting harm) above some "customary" level — before they are deemed unreasonable.

The FTC asserts that this standard is sufficiently well-defined, that LabMD's failure to engage in certain, specific actions enabled the data breach to occur, and thus that LabMD must have deviated from what was required of it. But a company cannot be faulted for engaging in conduct (or for failing to engage in conduct) that it does not know, or could not know, violates its duty of care. It is not the case that LabMD had *no* data security program. "LabMD

employed a comprehensive security program that included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections." Brief for Petitioner at 2, *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. Dec. 27, 2016) (citations to the record omitted). The Commission disputes some of these. But for every practice the FTC claims LabMD did *not* engage in, there were other practices in which it *did* engage.

The FTC simply has not established that LabMD's practices were insufficient to meet its duty of care. At best, the Commission has argued that LabMD failed to engage in *some* conduct that *could* be part of the duty of care. But even if LabMD failed to engage in every practice derived from FTC consent decrees (most of which post-date the relevant time period here), or some of the practices described in one or more of the industry standard documents that the FTC refers to, *see* FTC Opinion at 12 & n. 23, the FTC has failed to establish that LabMD's practices. *as a whole*, were insufficient to meet a reasonable standard of care. Even if LabMD failed to engage in *some* of the wide range of possible practices that comprise the FTC's (undefined) standard, the FTC still has not established that such a failure causes the overall data security regime to become insufficient.

Where, as here, the FTC focuses on the sufficiency of precautions relating to the specific harm that occurred, it fails to establish the requirements for an overall data protection scheme — the relevant consideration. The general security obligations under which any company operates prior to a specific incident are not necessarily tied to that incident. *Ex ante*, in implementing its security practices, LabMD would not have focused particularly on the P2P risk, which was, at the time, not particularly well understood. Before Tiversa's incursion, LabMD surely faced different security risks, and undertook to adopt measures to protect against them. Given this, the existence of P2P software on one computer in its billing department was hardly unreasonable, in light of the protections LabMD *did* adopt. Despite suffering no no security breaches, the Commission would invalidate all of LabMD's data protection measures because of the single (unlikely) breach that *did* occur.

The fundamental problem with the FTC's argument is that, by arguing backward solely from what eventually *did* occur, and failing to assess the *ex ante* risk that it *as well as all other possible security problems* would occur, the FTC puts the cart before the horse and effectively converts a negligence-like regime into one of strict liability. The duty of care that must be violated for a "reasonableness" standard is meaningless if it is defined solely by such a narrow, post hoc analysis. By effectively defining "reasonableness" in terms of a company's

failure to thwart only the breach that *did* occur (and not the ones that *could* have but did *not*), the analysis becomes one of effective strict liability.

B. The FTC Misinterprets the Plain Meaning of "Substantial Injury."

When establishing causality, Section 5(n) is not focused on the "substantial[ity]" of the injury; the *likelihood* that conduct caused substantial injury and the *substantiality* of the injury itself are distinct concepts. Conduct does not become more likely to *cause* harm in the first place just because the resulting harm may be relatively more *substantial.*

This is clear from the statute: "Substantial" modifies "injury," not "likely." Either conduct *causes* substantial injury, or it is *likely* to cause substantial injury, meaning it creates a heightened risk of substantial injury. To reimport the risk component into the word "substantial" following the word "likely" makes no syntactic sense: "Likely to cause" already encompasses the class of injuries comprising increased risk of harm. The FTC's interpretation would amount to creating liability for conduct that creates *a risk of a risk* of harm.

Although the Unfairness Statement does note that "[a]n injury may be sufficiently substantial… *if it raises a significant risk of concrete harm,*" FTC Opinion at 21 (quoting Unfairness Statement at 1073 n. 12) (emphasis added), "raises" clearly does not mean "increases the degree of" here, but rather "stirs up" or

"gives rise to." *Raise*, Merriam-Webster.com (last visited Jan. 2, 2017), *available at* https://goo.gl/R2sVhm. And the relevant risk in footnote 12 is deemed to be "significant," not "substantial," suggesting it was intended to be of a different character. Moreover, that passage conveys the Commission's intention to address inchoate harms under Section 5 — conduct "likely" to cause harm: In effect, footnote 12 was incorporated into Section 5(n) by inserting the words "or is likely to cause" in the phrase "causes… substantial harm." Importing it *again* into the determination of substantiality is a patently unreasonable reading of the statute and risks writing the substantial injury requirement out of the statute.

At first blush, the FTC's proposed multiplication function ("[A] practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low." FTC Opinion at 21) may sound like the first half of Footnote 12 ("An injury may be sufficiently substantial, however, if it does a small harm to a large number of people." Unfairness Statement at n.21), but these are two very different things. Indeed, the fact that the Footnote proposes a multiplication function for interpersonal aggregation of harms, but then, in the next breath, says no such thing about multiplying small risks times large harms, can have only one meaning: The Policy Statement requires the FTC to prove the substantiality of harm, independent of its risk. Had Congress

intended for the rather straightforward strictures of 5(n) to accommodate the large loophole proposed by the FTC, it surely would have spoken affirmatively. It did not. Instead, as is evident from the plain text of the statute, Congress structured Section 5(n) as a meaningful limitation on the FTC's potentially boundless Unfairness authority.

The Commission claims that "[t]he Third Circuit interpreted Section 5(n) in a similar way in *Wyndham*. It explained that defendants may be liable for practices that are likely to cause substantial injury if the harm was 'foreseeable,' … focusing on both the 'probability and expected size' of consumer harm." FTC Opinion at 21 (internal citations omitted). But the *Wyndham* court did *not* declare that the first prong of Section 5(n) requires that the magnitude of harm be multiplied by the probability of harm when evaluating its foreseeability. Instead, the court includes the magnitude of harm as one consideration in cost-benefit analysis:

> [T]his standard informs parties that the relevant inquiry here is a cost-benefit analysis … that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.

Wyndham, 799 F.3d at 255 (internal citations omitted). This is not the same as the Commission's proffered approach. The Third Circuit essentially recited the

elements of a complete evaluation of Section 5(n), *not* the requirements for evaluating the first prong of the test.

C. The FTC Failed to Demonstrate that LabMD's Conduct Caused or Was Likely to Cause Substantial Harm

Even with respect to causation, the Commission failed to adequately show that the actual and likely harm of which it complained was a foreseeable result of LabMD's conduct, given the standards (or lack thereof) of reasonable conduct in 2007.

There is some question whether the Act contemplates conduct at all that merely facilitates (or fails to prevent) harm by third parties, rather than causes harm to consumers directly. *See generally* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008). But even if the FTC does have authority to police data breaches and data security problems, *see, e.g.*, *Wyndham*, 799 F.3d at 248–49, the fit between such conduct and Section 5 remains uneasy.

The FTC has traditionally used its unfairness power to police coercive sales and marketing tactics, unsubstantiated advertising, and other mirepresentations to consumers; in such cases, there is a more direct line between conduct and harm. *See generally* Richard Craswell, *Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WISC. L. REV 107 (1981). In data secu-

rity cases, however, the alleged unfairness is a function of a company's failure to take precautions sufficient to *prevent* a third party's intervening, harmful action (*i.e.*, hacking).

This creates far more significant problems of causation and proof. While a company's security *may* have facilitated a breach, it is difficult to *know* whether this is true. The FTC simply infers causation from the existence of a breach. *See* Transcript of Closing Arguments (Rough Draft) at 48*, In re LabMD, Inc.,* F.T.C. Docket No. 9357 (Sep. 16, 2015) (on file with the authors) ("[Y]ou haven't cited any Court of Appeals case… [finds]… evidence of… a single breach, is sufficient to sustain a violation of *Section* 5"). But, as noted (and as the Commission recognizes elsewhere), no security can be perfect, and thus the fact of a breach cannot, *per se,* prove that a company's data security practices violated Section 5. Indeed, by the same token, even if a company *had* done everything the FTC asserts is required, there could *still* have been a breach. Instead the statute demands demonstration that the failure to prevent a breach violated the duty of care and that it *resulted in* — *i.e.*, was not *itself* — "substantial injury."

The FTC has failed to establish either that LabMD "cause[d] or [was] likely to cause substantial injury to consumers," or that its conduct was "not outweighed by countervailing benefits to consumers or to competition."

The Commission "does not know," FTC Opinion at 17, whether any patient encountered a single problem related to the breach, and thus has not articulated any injury caused by LabMD's conduct.[3] The Commission asserts that mere exposure of information suffices to establish harm. *See* FTC Opinion at 18 ("Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers"). But this amounts to saying that any conduct that causes breach causes harm. That not only violates the FTC's own claims that breach alone is not enough, it is patently insufficient to meet the substantial injury requirement of Section 5(n). The examples it adduces to support this point all entail not merely exposure, but actual dissemination of personal information to large numbers of unauthorized recipients who *actually read* the exposed data. *See generally In the Matter of MTS, Inc.* Dkt. No C-4110, 137 F.T.C. (2004), *available at* https://goo.gl/4emzhY (Tower Records liable for software error that allowed 5,225 consumers' billing information to be read by anyone, which actually occurred). Even if it is reasonable to assert in such circumstances that "embarrassment or other negative

[3] And although the Commission effectively blames LabMD for its (the FTC's) lack of knowledge of harm, that burden does not rest with LabMD. Moreover, the Commission had ample opportunity to collect such evidence if it existed, *e.g.*, by actually asking at least a sample of patients whose data was in the 1718 file or subpoenaing insurance companies to investigate possible fraud. That the Commission still cannot produce any evidence suggests, in the strongest possible terms, that none exists.

outcomes, including reputational harm" result from that sort of public disclosure, FTC Opinion at 17, no such disclosure occurred here. That the third-party responsible for exposure of data itself viewed the data — which is effectively all that happened here — cannot be the basis for injury without simply transforming the breach itself into the injury.

Moreover, instead of establishing a causal link between LabMD's conduct and even the breach itself (let alone the alleged harm), the FTC offers a series of *non sequiturs*, unsupported by evidence. The Order cites allegedly deficient practices, *see, e.g.*, FTC Opinion at 2, but establishes no causal link between these and Tiversa's theft of the 1718 file — nor *could* it, because the theft had nothing to do with passwords or operating system updates, or firewalls, and because things like integrity monitoring and penetration testing, at best, "'might have' aided detection of the application containing the P2P vulnerability," Pet. Br. at 47 (citations to the record omitted); *see also id.* at 31 & n. 13, LabMD's alleged failure to do these things cannot be said to have caused the (alleged) harm. Even with respect to other security practices that *might* have a more logical connection to the breach (*e.g.*, better employee training), the Commission offers no actual evidence demonstrating that these actually caused, or even were likely to cause, any harm.

Whatever the standard for "unreasonableness," there must be a causal connection between the acts (or omissions) and the alleged injury. Even for likely harms this requires not mere possibility but *probability* at the time the conduct was undertaken. *See* Initial Decision at 54. Instead, the Commission merely asserts that harm was sufficiently "likely" based on its own *ex post* assessment, in either 2012 or 2016, of the risks of P2P software in 2007.

The FTC's Chief Administrative Law Judge found this assertion wanting, ruling that the Commission had failed to establish likely harm. *Id.* at 53. But the Commission, in its turn, disagreed:

> The ALJ's reasoning comes perilously close to reading the term "likely" out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes.

FTC Opinion at 23. This is true, as far as it goes, but the FTC's only evidence on the likelihood of harm in 2007 is… evidence of the likelihood of such harm in 2013 and today. *Id.* at 24. Moreover, judgments about the likelihood that past conduct will cause harm must be informed by what has actually occurred. By the time the FTC filed its complaint, and surely by the time the FTC rendered its opinion, facts about what actually happened up to that point should have informed the Commission about what was likely to occur. That the only

available facts point to the complete absence of injury suggests injury was not likely caused by any of LabMD's conduct.

It is thus the Commission that is in danger of reading "likely" out of the statute — and "substantial" for that matter. Under the FTC's interpretation the statute could have been written as "The Commission shall have no authority under this section… to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or [could conceivably have] cause[d]… [any] injury."

CONCLUSION

For the foregoing reasons, the FTC's Order should be vacated.

Respectfully submitted,

Geoffrey A. Manne
Kristian Stout
INTERNATIONAL CENTER
FOR LAW & ECONOMICS
3333 NE Sandy Blvd., Suite 207
Portland, OR 97232
503-770-0076
gmanne@laweconcenter.org

Berin M. Szóka
Thomas W. Struble
TECHFREEDOM
110 Maryland Avenue, Suite 409
Washington, DC 20002
202-803-2867
bszoka@techfreedom.org

John P. Hutchins*
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
(404) 267-2733 Direct
(404) 267-2750 Fax
(404) 644-9325 Mobile
John.Hutchins@leclairryan.com
https://www.leclairryan.com

* Counsel of Record

January 3, 2017

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies that this brief complies with Fed. R. App. P. 32(a) because, excluding the parts exempted by Fed. R. App. P. 32(f) and 11th Cir. R. 32-4, this brief contains 6,478 words and has been prepared in a 14-point proportionally spaced typeface.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

CERTIFICATE OF SERVICE

I hereby certify that, on January 3, 2017, I filed the foregoing document in the United States Court of Appeals for the Eleventh Circuit using the Court's Electronic Case Files (ECF) system, which generates a notice that is emailed to attorneys of record registered to use the ECF system.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

UNIVERSITY OF CALIFORNIA
HASTINGS COLLEGE OF THE LAW

LEGAL STUDIES RESEARCH PAPER SERIES

Research Paper No. 265

NO ONE OWNS DATA

Lothar Determann
ldetermann@bakernet.com

70 Hastings Law Journal (2018 forthcoming)

1st Draft Feb. 14, 2018
2nd Draft March 14, 2018
3d Draft August 8, 2018

NO ONE OWNS DATA

by Lothar Determann[1]

Thoughts are free.
Who can guess them right?
They fly by me, like shadows at night.
No one can mute them.
No hunter can shoot them.
It remains for all to see:
Thoughts are free.
(German folk song)[2]

---

[1] Lothar Determann teaches computer, internet and data privacy law at Freie Universität Berlin, University of California, Berkeley School of Law and Hastings College of the Law, San Francisco, and he practices technology law as a partner at Baker McKenzie LLP in Palo Alto. Opinions expressed in this article are those of the author, and not of his firm, clients or others. The author is grateful for valuable input, research and edits by Yoon Chae, Thomas Blickwedel, Paloma Pietsch and Shemira Jeevaratnam, as well as additional suggestions from Prof. Eric Goldman, Santa Clara University School of Law, and Tony Bedel.

[2] German folk song. Lyrics in German: "Die Gedanken sind frei. Wer kann sie erraten. Sie fliegen vorbei, wie nächtliche Schatten. Kein Mensch kann sie wissen, kein Jäger sie schießen. Es bleibet dabei: Die Gedanken sind frei." The original lyricist and composer are unknown, but the most popular version was rendered by Hoffmann von Fallersleben in 1842. *See Die Gedanken sind frei*, DEUTSCHLAND-LESE, http://www.deutschland-lese.de/index.php?article_id=110 (all hyperlinks in this Article were last visited Jan. 23, 2018) (Ger.).

I. INTRODUCTION

Connected cars, industrial machines, toys and other devices on the Internet of Things (IoT) generate vast amounts of data and information. The total amount of stored data is expected to double every two years—meaning a 50-fold growth from 2010 to 2020[3]—and reach 163 zettabytes by 2025.[4] Autonomous vehicles, for example, can each generate as much as 4,000 gigabytes of data every day[5] on the vehicle's performance and maintenance, location of the car, and various aspects of the people in the car[6] with the help of today's advanced sensors.[7]

The explosive growth in the total amount of data will come from technologies that were both historically inside and outside of cars, fueled by the high level of forecasted interconnectivity of nearly all devices.[8] Existing in-vehicle technologies, such as in-dash navigation systems, diagnostic systems, and virtual assistants already generate data[9] and will

---

[3] PETER FFOULKES, THE INTELLIGENT USE OF BIG DATA ON AN INDUSTRIAL SCALE 2 (2017), https://insidebigdata.com/white-paper/guide-big-data-industrial-scale.

[4] DAVID REINSEL, JOHN GANTZ & JOHN RYDNING, DATA AGE 2025: THE EVOLUTION OF DATA TO LIFE CRITICAL 3 (2017), https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

[5] Patrick Nelson, *Just One Autonomous Car Will Use 4,000 GB of Data/Day*, NETWORK WORLD (Dec. 7, 2016), https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html.

[6] MCKINSEY & CO., MONETIZING CAR DATA REPORT 8 (2016), https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Creating%20value%20from%20car%20data/Creating%20value%20from%20car%20data.ashx.

[7] These sensors include global positioning systems (GPS), dedicated short-range communications devices (DSRCs), light detection and ranging sensors (LIDAR), cameras, infrared sensors, and radio detection and ranging (RADAR) devices. *See* AUTONOMOUS VEHICLES, CTR. FOR SUSTAINABLE SYS., UNIV. OF MICHIGAN (Aug. 2017), http://css.umich.edu/sites/default/files/Autonomous_Vehicles_Factsheet_CSS16-18_e2017.pdf. They play evermore important roles in safety and technological advancements in vehicles and other connected devices today. *See* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 1, 16-18 (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837598.

[8] The number of devices connected to IoT will soon exceed the number of people on earth. *See* G.V. Sam Kumar, *Survey on Process in Scalable Big Data Management Using Data Driven Model Frame Work*, 5 INT'L J. OF INNOVATIVE RES. IN COMPUTER & COMM. ENGINEERING 4468, 4469 (2017).

[9] *See* Matthew DeBord, *Big Data in Cars Could Be $750 Billion Business by 2030*, Business Insider (Oct. 3, 2016, 4:08 PM), http://www.businessinsider.com/car-data-business-mckinsey-and-co-report-2016-10.

continue to do so at an accelerated rate. Features such as voice controls will be used for more applications, while both video and audio will be recorded in more places.[10] Use of biometric data will become more prevalent for authentication in various devices, including cars and other IoT devices,[11] and technologies usually reserved for healthcare, such as heart rate monitors, will likely be incorporated into vehicles to assess the passengers' health risks and ride comfort.[12]

Various parties are actively staking their claims to data on the Internet of Things, as they are mining data, the fuel of the digital economy. The data generated is valuable to various persons and entities for different reasons, including safety, risk assessments, compliance, preventive maintenance, market intelligence, development of new business models, public policy, and law enforcement, among others.[13] But much of the sought-after data will relate to personal and private information of various individuals (*e.g.*, regarding their health, travel history and speed, browsing history, and emails),[14] which raises privacy concerns and questions of who may access and use the data generated by the various connected things. These questions are often framed as issues of *data ownership* or *property*

---

10 *See* Jordan Novet, *Google's Self-Driving Cars Could Come with Gesture-Based Controls, Pedestrian Notifications*, VENTURE BEAT (Mar. 3, 2015), https://venturebeat.com/2015/03/03/googles-self-driving-cars-could-come-with-gesture-based-controls-pedestrian-notifications/.

11 *See* Salil Prabhakar, *Why Biometrics Are the Key to Driver Authentication in Connected Cars*, VENTURE BEAT (Feb. 7, 2017), https://venturebeat.com/2017/02/07/why-biometrics-are-the-key-to-driver-authentication-in-connected-cars; John Trader, *5 Ways Biometric Technology is Used in Everyday Life*, M2SYS BLOG (Sept. 24, 2013), http://www.m2sys.com/blog/guest-blog-posts/5-ways-biometric-technology-is-used-in-everyday-life.

12 *See also* MCKINSEY & CO., MONETIZING CAR DATA REPORT 7 (2016), https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Creating%20value%20from%20car%20data/Creating%20value%20from%20car%20data.ashx (discussing people's willingness to share data on fitness and health).

13 David Welch, *Your Car Has Been Studying You; Everyone Wants the Data*, Bloomberg BNA Privacy & Security Law Report 15 PVLR 1482 (July 12, 2016). Data is an enabler of business models of the future *e.g.*, the convergence of car manufacturers, rental car companies, transportation businesses, ride share ventures and others to "mobility providers."

14 *See* McKinsey & Company, Car Data: Paving the Way to Value-Creating Mobility 7-9 (2016).

rights in data in the popular press and political discussions.[15] Businesses, politicians and scholars assume the existence of or call for the creation of property rights in data.[16] Yet, in the context of this debate there is much uncertainty and ambiguity regarding the meaning of "data," "information," and "ownership;" little comprehensive analysis regarding how existing property laws already cover data or exclude data from protection; and relatively sparse considerations of legal and policy reasons for *not* granting property rights to data.

This Article comprehensively examines and decidedly challenges assumptions regarding the existence or policy reasons for ownership rights in data and argues that data (1) exists separately from works of authorship, databases, and media (*see infra* Part II); (2) is largely free from property rights (*see infra* Part III); (3) is subject to a complex landscape of access rights and restrictions (*see infra* Part IV); and (4) implicates various legal positions, interests, and options for parties interested in the data that are regulated in a considerate, nuanced, and balanced fashion under laws outside the property law realm (*see infra* Part V). The Article then examines current policy discussions around the creation of a right to data

---

15 *See, e.g.*, Evgeny Morozov, *To Tackle Google's Power, Regulators Have to Go After Its Ownership of Data*, THE GUARDIAN (July 2, 2017), www.theguardian.com/technology/2017/jul/01/google-european-commission-fine-search-engines.

16 . *See, e.g.*, Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2059 (2004); Lawrence Lessig, The Architecture of Privacy, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (1999); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, (1999), p. 122-35; Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM Sept. 1996, p. 92; Catherine M. Valerio Barrad, *Genetic Information and Property Theory*, 87 NW. U. L. REV. 1037, 1062-63 (1993); Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 964 (2012); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2383 (1996); James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 UNIV. OF TORONTO L.J. 183 (2004); Herbert Zech, "Industrie 4.0" - Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151, 1160; Karl-Heinz Fezer, Dateneigentum der Bürger, ZD 2017, 99; Janeček, Václav, Ownership of Personal Data in the Internet of Things (December 1, 2017). Computer Law & Security Review, 2018, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3111047 or http://dx.doi.org/10.2139/ssrn.3111047. *But see* Pamela Samuelson, *Symposium: Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); Louisa Specht, Ausschließlichkeitsrechte an Daten - Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 268.

ownership (*see infra* Part VI) and concludes that no one does or should be able to own data (*see infra* Part VII). The legal standards and frameworks employed in the Article are discussed from both U.S. and European perspectives to address the significant differences in transatlantic data privacy and data base protection law.[17] To develop and illustrate these theses, the Article refers to the landscape of interests in data generated or processed by connected cars and other devices on the IoT, which are driving current economic developments and policy discussions, including calls from the German government for a statutory property regime assigning rights to data from cars to auto manufacturers.[18]

II. DATA AND INFORMATION

In everyday parlance, the terms "data" and "information" are often used synonymously,[19] referring to "facts about a situation, person, [or] event."[20] "Data" and "information" are also used interchangeably in various legal contexts.[21] Likewise, this Article uses "data" and

---

17 *See generally* Paul M. Schwartz, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017) (discussing the differences in transatlantic data privacy law and the business reasons behind those differences).

18 Bundesministerium für Verkehr und digitale Infrastruktur, "Eigentumsordnung" für Mobilitätsdaten, www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html; Gerrit Hornung/Thilo Goeble, "Data Ownership" im vernetzten Automobil, CR 2015, 265, 272.

19 *See, e.g.*, *Data*, MERRIAM WEBSTER DICTIONARY, www.merriam-webster.com/dictionary/data (last visited Jan. 23, 2018).

20 *See, e.g.*, *Definition of Information*, CAMBRIDGE ADVANCED LEARNER'S DICTIONARY & THESAURUS, https://dictionary.cambridge.org/us/dictionary/english/information (last visited Jan. 23, 2018).

21 In the U.S., for example, the Fair Credit Reporting Act defines "medical information" as "information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer." Under EU data protection laws, "personal data" refers to "any information relating to an identified or identifiable natural person." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1, 33 (hereinafter GDPR).

"information" interchangeably, cognizant of different approaches to terminology in other academic disciplines.[22]

Information can be or relate to diverse things, such as memories, thoughts, discoveries, insights, opinions, perceptions, fictions, or answers to questions.[23] Information can be stored in physical forms, such as human brains and data servers, or physically expressed in books or on road markings. It can also be communicated via smoke signals, blinking lights, measurable radio waves, digital cable connections or writings on a wall. But the informational content, *i.e.*, data as such, exists separately from its context of a larger data base or work of authorship or its physical embodiment; for example, informational content of a smoke or light signal, photo, or painting may convey a message that "a dangerous machine is approaching,"[24] which would exist separately from its tangible manifestation (*e.g.*, smoke signal, photo, or painting), any creative expression (*e.g.*, text or painting) and the physical means through which it is perceived (*e.g.*, human eyes, ears or brains).

Consequently, different persons could assert different rights and interests in (1) informational content (*e.g.*, a dangerous machine is approaching), (2) expression of information in words, symbols, paintings,

---

22 Some data scientists use the term "data" to refer to discrete, objective facts or observations, which are unorganized, unprocessed and without any specific meaning, and the term "information" to refer to data that has been shaped into forms that are meaningful and useful to human beings. *See* Saša Baškarada & Andy Koronios, *Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*, 18 AUSTRALASIAN J. OF INFO. SYS. 7 (2013) (internal citations omitted). Data can thus be considered as patterns with no meaning, whereas information refers to interpreted data that has meaning. *Id.* at 7; *see also* Mireille Hildebrandt, *Law as Computation in the Era of Artificial Legal Intelligence*, UNIV. OF TORONTO L.J. 1, 3 (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2983045 (citing Mireille Hildebrandt, *Law as Information in the Era of Data-Driven Agency*, 79 MODERN L.R. 1, 1-33 (2016)). For a discussion on further distinctions between "data" and "information," as well as their distinctions with "knowledge" and "wisdom," generally see Saša Baškarada & Andy Koronios, *Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*, 18 AUSTRALASIAN J. OF INFO. SYS. (2013). *See also* the illustrated discussion of definitions at www.datenschutzbeauftragter-online.de/daten-information-definition/.

23 *See Information*, DET INFORMATIONS-VIDENSKABELIGE AKADEMI, http://www.informationsordbogen.dk/concept.php?cid=902 (last visited Jan. 23, 2018) (Ger.)

24 This informational content further comprises a factual assertion (*i.e.*, an animal is approaching) and an assessment (*i.e.*, the animal is dangerous).

or other works of authorship, or compilations or data bases in which information is organized creatively or functionally, and (3) physical manifestation of information (*e.g.*, smoke signal, photo, painting on a wall), as well as (4) the item to which the information relates (*e.g.*, malfunctioning autonomous vehicle or other machine). Ownership and property rights in these different aspects and embodiments of data or information are explored under different property law regimes in Part III.

III. PROPERTY RIGHTS IN DATA

A. OWNERSHIP AND PROPERTY RIGHTS

"Ownership" generally refers to "the right to exclusive use of an asset"[25] or "the full right to dispose of a thing at will."[26] Ownership assigns a thing to a person or legal entity and signifies that the object belongs to that person.[27] We also use the term "ownership" more broadly in everyday language with respect to owning an ability or responsibility,[28] where one can "own up to" having done something.[29]

In U.S. law, ownership denotes property rights, referring to a "bundle of rights allowing one to use, manage, and enjoy property, including the right to convey it to others,"[30] as well as the rights of "exclusive use or monopoly over the property owned."[31] Similarly, German law defines "ownership" in reference to an owner's ability to "deal with [a] thing at

---

25 NIGAR HASHIMZADE, GARETH MYLES & JOHN BLACK, A DICTIONARY OF ECONOMICS (5th ed. 2017).

26 THE OXFORD DICTIONARY OF BYZANTIUM (Alexander P. Kazhdan ed., 1991).

27 *See* OXFORD DICTIONARY OF ENGLISH 1270 (3d ed. 2010) (definition of "own").

28 *See, e.g.*, *Meaning of "ownership" in the English Dictionary*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/ownership#translations (last visited Jan. 23, 2018) (additionally defining "ownership" as "the fact of taking responsibility for an idea or problem").

29 *See, e.g.*, *Meaning of "own up" in the English Dictionary*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/own-up (last visited Jan. 23, 2018) (under English tab) ("To admit that you have done something wrong."); *id.* (under American tab) ("To tell the truth or to admit that you are responsible for something.")

30 BLACK'S LAW DICTIONARY 1280 (10th ed. 2009).

31 Stephen M. Sheppard, *Ownership (Owner or Own)*, THE WOLTERS KLUWER BOUVIER LAW DICTIONARY (2012).

his discretion and exclude others from every influence," as long as it does not come into conflict with a statute or third-party rights."[32]

Correspondingly, "property" refers to "everything that is owned" or "subject of ownership."[33] Three main categories of property are *real* property (*e.g.*, land or real estate),[34] *personal* property (*i.e.*, physical property other than real property),[35] and *intellectual* property[36] (*e.g.*, intangible property based on ideas).[37]

Property rights entail a set of rules that govern people's access to and control of property,[38] and the "bundle of rights" [39] that the owner can hold

---

[32] BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], Aug. 18, 1896, REICHSGESETZBLATT [RGBL.] 195, amended Oct. 1, 2013, BGBL. I at 3719, § 903 (Ger.), *translated in* GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html (last visited Jan. 23, 2018) [hereinafter GER. CIV. CODE].

[33] *property*, THE LAW DICTIONARY (2002) (from LexisAdvance search); *Property*, THE FREE DICTIONARY – LEGAL DICTIONARY, https://legal-dictionary.thefreedictionary.com/property (last visited Jan. 28, 2018).

[34] *See real property, real estate, or realty*, THE LAW DICTIONARY (2002) (from LexisAdvance search) ("Real property includes land and any interest or estate in land."); *see also* BLACK'S LAW DICTIONARY 1412 (10th ed. 2009) (defining immovable property as "land and anything growing on, attached to, or erected on it, excluding anything that may be severed without injury to the land.").

[35] *See personal property*, THE LAW DICTIONARY (2002) (from LexisAdvance search) ("Anything which is subject to ownership and which is not a freehold in real property."); *see also* BLACK'S LAW DICTIONARY 1412 (10th ed. 2009) (defining movable property as "any movable or intangible thing that is subject to ownership and not classified as real property.").

[36] Intellectual property refers to "a category of intangible rights protecting commercially valuable products of the human intellect." BLACK'S LAW DICTIONARY, 930 (10th ed. 2009). For a discussion on how intellectual property, such as trade secrets, copyrights, patents, and trademarks, also qualify as "property," see Brian M. Hoffstadt, *Dispossession, Intellectual Property, and the Sin of Theoretical Homogeneity*, 80 S. Cal. L. Rev. 909, 910 (2007).

[37] Jade McKenzie, *Comment: Em"BARK"ing on the Journey to Expand Recovery of Damages for the Loss of a Companion Animal*, 19 CHAP. L. REV. 659, 663 (2016); *see also* David Favre, *Living Property: A New Status for Animals Within the Legal System*, 93 MARQ. L. REV. 1021, 1025-1026 (2010) ("The standard discussion of property today lists three basic categories of property – real property, personal property, and intellectual property. . . . Real property is fixed in place, visible for all to see and will last indefinitely. . . . Personal property is physical, moveable, and has a limited physical existence. . . Intellectual property is a product of a human mind.")

[38] Jeremy Waldron, *Property and Ownership*, *in* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY 2 (Edward N. Zalta ed., 2016).

[39] Other theories for defining property include the exclusivity theory, where exclusivity rights are the sole requirement for property, and the integrated theory, which

against others, including (1) the right to possess, (2) the right to exclude,[40] and (3) the right to transfer.[41] Among the three, the right to *exclude* is described as "one of the most essential sticks in the bundle of rights that are commonly characterized as property."[42]

Contracts, torts, competition, and penal laws can also convey exclusion rights, but not a complete bundle of rights that amounts to ownership. Contracts can mimic all rights typically conferred by property laws, but create rights and obligations only between contracting parties and named beneficiaries. Companies often agree in contracts that one party shall own certain data. But, such an agreement binds only other contracting parties and not anyone else, and can thus not convey actual property rights. Torts, competition, and penal laws can generally prohibit

---

states that exclusivity is not enough and looks at how the asset is acquired, used and disposed. *See* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 16-18 (2007). This Article prefers the bundle of rights theory to address ownership and property rights in data, as it provides more flexibility for addressing data ownership under different property law regimes. *Id.* at 18 ("The middle ground is . . . 'Hohfeldian' bundle of rights.")

[40] *See* J. E. Penner, *The Bundle of Rights Picture of Property*, 43 UCLA L. REV. 711, 713 (1996) ("[T]he right to possess, the right to use, the right to capital, the liability to execution, the immunity from expropriation, and so on."); Stephen M. Sheppard, *Property Right (Property Rights)*, THE WOLTERS KULWER BOUVIER LAW DICTIONARY (2012) (referring property rights as "the rights of ownership, possession, and use of lands, things, and ideas, including intellectual property."); *see also* RICHARD A. EPSTEIN, TAKINGS: PRIVATE PROPERTY AND THE POWER OF EMINENT DOMAIN 35-104 (1985) (explaining that the "bundle of rights" approach has become the standard starting point for an inquiry into the nature of property); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) ("[B]undle of rights that are commonly characterized as property.").

[41] Tom W. Bell, *"Property" in the Constitution: The View From the Third Amendment*, 20 WM. & MARY BILL RTS. J. 1243, 1250 (2012) ("Unless 'property' comes with a limiting adjective, then, it covers anything of value subject to an owner's exclusive rights of use and transfer."); Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) ("Of course, those who are given the right to exclude others from a valued resource typically also are given other rights with respect to the resource – such as the right . . . to transfer it").

[42] *Kaiser*, 444 U.S. at 176; *see also* Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 754 (1998) ("[T]he right to exclude others is more than just 'one of the most essential' constituents of property – it is the sine qua non."). The U.S. Supreme Court has also focused on the right to exclude in its interpretation of the Fourth Amendment of the Constitution. *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security*, 33 WAKE FOREST L. REV. 307 (2009); *see also United States v. Jones*, 132 S. Ct. 945 (2012) (discussing that the Court's Fourth Amendment jurisprudence used to be tied to common-law trespass, but that its later cases have deviated from that exclusively property-based approach).

data access or use except by authorized persons and thus create *de facto* exclusion rights.[43] But, torts, competition, and penal laws are limited to prohibitions and do not convey rights to possession, access, use, and alienability to the authorized person who is exempt from the prohibitions; such laws are intended to prohibit conduct that is harmful to society, business integrity, or individual freedoms and stop short of creating property.

Governments grant ownership and property rights primarily for utilitarian or economic incentive reasons.[44] Property rights are thus granted to incentivize creations or improvements of property, such as farm land (real property) and chattels (personal property),[45] as well as various intangibles,[46] including works of authorship (copyrights),[47] brands

---

43 Such as the U.S. Computer Fraud and Abuse Act and other computer interference laws, unfair competition laws, data privacy laws, trade secrt laws and database protection laws.

44 ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 11 (6th ed. 2012); *see also* Eric A. Posner & E. Glen Weyl, *Property is Only Another Name for Monopoly*, 9 J. OF LEGAL ANALYSIS 51, 51 (2017) ("Property rights of all sorts—in real estate, in shares of corporations, and in radio spectrum, to take three diverse examples—give the owner a monopoly over a resource. It is conventional to think that this monopoly is benign. It gives the owner an incentive to invest in improving the property because she receives the entire payoff from its use or sale. This aligns social and private incentives for investment in property."); PETER HORSLEY, PROPERTY RIGHTS VIEWED FROM EMERGING RELATIONAL PERSPECTIVES 89 (2011) ("Property rights encourage property holders to develop their property, generate wealth, and efficiently allocate resources based on the operation of the market.") Other theories for justifying property rights are the natural rights perspective, as advanced by John Locke in *Two Treatises on Government*, and the personhood justification, as developed by Georg Wilheim Freidrich Hegel in *Philosophy of Right*. For further discussions on the natural rights perspective, see Jeremy Waldron, *Property and Ownership*, *in* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY 10 (Edward N. Zalta ed., 2016), Donna M. Byrne, *Locke, Property, and Progressive Taxes*, 78 NEB. L. REV. 700, 705 (1999), and Carol M. Rose, *Possession as the Origin of Property*, 52 U. CHI. L. REV. 73, 73 (1985). For further discussions on the personhood justification, see Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 971 (1982).

45 *See, e.g.*, GER. CIV. CODE §§ 99 & 953 (stating that property rights are granted to the owner of the thing); CAL. CIV. CODE § 658 (generally granting property rights in crops to the owner of the land).

46 *See, e.g.*, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, art. 1, 2004 O.J. (L 195/16) 1, 1 ("The protection of intellectual property is important not only for promoting innovation and creativity, but also for developing employment and improving competitiveness."); *id.* at art 2, 2004 O.J. (L 195/16) 1, 1 ("The protection of intellectual property should allow the inventor or creator to derive a legitimate profit from his/her invention or creation. It should also allow the widest possible dissemination of works,

(trademarks), and inventions (patents).[48] For these types of creations, in which the real value lies in their intangible aspects, governments grant property rights to reward and incentivize the creators and inventors by allowing them to monetize their creations and exclude their competitors (or make them license the rights for a fee or rent).[49]

As governments extend property rights to reward investment and innovation, they also must consider various conflicting interests of the public. Property laws need to evolve in pace with societal and technological changes.[50] The arising rights should be granted only if they

---

ideas and new knowhow. At the same time, it should not hamper freedom of expression, the free movement of information, or the protection of personal data, including on the Internet.").

47 *See, e.g.*, Cal. Civ. Code §§ 654-1422; 17 U.S.C. §§ 101-1332 (2012); Ger. Civ. Code §§ 903-1011; Urheberrechtsgesetz [UrhG] [Act on Copyright and Related Rights], Sept. 9, 1965, BGBl. I at 1273, amended Dec. 20, 2016, BGBl. I at 3037 (Ger.), translated in Gesetze im Internet, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018) [hereinafter German Copyright Act].

48 *See, e.g.*, 35 U.S.C. § 101 (2012) ("Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title"); PATENTGESETZ [PATG] [PATENT ACT], Dec. 16, 1980, BGBL. I at 1, amended Oct. 19, 2013, BGBL. I at 3830 (Ger.), translated in WIPO, http://www.wipo.int/wipolex/en/text.jsp?file_id=401424 (last visited Jan. 23, 2018). The four major economic justifications for patent law, according to a 1966 Report of the President's Commission on the Patent System, are that the patent system (1) provides an incentive to invent, (2) stimulates the investment of additional capital needed for the further development and marketing of the invention, (3) encourages early public disclosure of technological information, and (4) promotes the beneficial exchange of products, services, and technological information. *See* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 17 (6th ed. 2012) (citing COMMITTEE ON THE JUDICIARY OF THE UNITED STATES SENATE, REPORT OF THE PRESIDENT'S COMMISSION ON THE PATENT SYSTEM 2 (1966)).

49 *See* U.S. CONST. art. I, §8, cl. 8 (granting Congress the power to enact copyright laws in order to "promote the Progress of Science and useful arts.") and, *e.g.*, Thomas Jefferson, WRITINGS 333 (1905) ("Society may give an exclusive right to the profits arising from them, as an encouragement to men to pursue ideas which may produce utility, but this may or may not be done, according to the will and convenience of the society, without claim or complaint from anybody.")

50 *See Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1069 (1992) ("Arresting the development of the common law is not only a departure from our prior decisions; it is also profoundly unwise. The human condition is one of constant learning and evolution -- both moral and practical. Legislatures implement that new learning; in doing so they must often revise the definition of property and the rights of property owners.").

do not come into conflict with existing laws and third-party rights.[51] The rights to use and exclude are thus restricted in various ways. For example, landowners' rights are limited by the right of way for neighbors under certain circumstances,[52] and their rights to use are further limited by land development regulations, gun control laws, and traffic rules, among others.[53]

Proper limits need to be established for intellectual property laws as well. Although designed to incentivize investments for the greater good, such as for stimulating scientific and technological progress or developing the fine arts, exclusivity rights that are granted too broadly or for too long can actually impair the desired progress.[54] This is why limitations, carve-outs, and exceptions have been set for intellectual property rights, so that a balance can be established between the interests of innovators and of the wider public. Data is typically one of the carve-outs from protectable subject matter definitions in intellectual property laws,[55] and there is no known "data property statute" in any country.

Yet, various existing property law regimes implicate data and information in different aspects, forms, and scenarios, as discussed in the subsequent sections of Part III, although none of those regimes grant any effective ownership or property rights in the data itself. The subsequent

---

51 *See, e.g.*, GER. CIV. CODE § 903 ("[O]wner of a thing may, to the extent that a statute or third-party rights do not conflict with this, deal with the thing at his discretion and exclude others from every influence.").

52 *See, e.g.*, GER. CIV. CODE § 917(1) ("If a plot of land lacks the connection to a public road necessary for the due use, the owner may require of the neighbors that until the defect is removed they tolerate the use of their plots of land to create the necessary connection."); *see also* CAL. CIV. CODE § 1009.

53 *See* GER. CIV. CODE § 903 ("The owner of an animal must, when exercising his powers, take into account the special provisions for the protection of animals.").

54 *See, e.g.*, Peter Lee, *Symposium: Chief Judge Radar's Contribution to Intellectual Property Law and Practice*, 7 WASH. J.L. TECH. & ARTS 405, 417 (2012) ("In that context, separating protectable expression from nonprotectable idea often proceeds as a policy determination inquiring into whether an asset is so abstract that subjecting it to exclusive rights would effectively impair rather than advance creative progress."); ELEC. FRONTIER FOUNDATION, *Defend Innovation*, https://web.archive.org/web/20151222074452/https://defendinnovation.org/proposals (last visited on Jan. 28, 2018) (asserting that a "patent covering software should be shorter; no more than five years from the application date" so that the patent system can defend innovation, instead of hindering it).

55 Patent law excludes laws of nature, natural phenomea and abstract ideas from patentable subject matter, trade mark law denies protection for generic marks and copyright law excludes facts and ideas from copyright protection in 17 U.S.C. § 102(b).

sections of Part III also explore the popular justifications and legal frameworks for property rights under each property law regime to provide the analytical framework for assessing potential policy reasons for creating new property rights in data.

B. REAL PROPERTY

Real property laws may grant ownership rights to physical manifestations of information that attach to real property, but do not provide any ownership rights to the underlying information itself. Real property laws are designed to protect land and anything that grows on or is permanently attached to or erected on that land, including buildings, crops, mines, roads, and machinery.[56] Owners are entitled to the real property's access, use, possession, enjoyment, disposition, and exclusion of others (trespassers),[57] as well as to harvest its crops, fruits, game, water, and minerals. These ownership rights, however, are limited in different aspects. For example, the owner must comply with building codes and

---

[56] *See Story v. Christin*, 95 P.2d 925 (Cal. 1939) ("Under common law, whatever was attached to land in any manner, including plants and trees growing in soil, as well as buildings and other products of man's labor, was part of the land."); *Kindig v. Palos Verdes Homes Ass'n*, 91 P.2d 645 (Cal. Ct. App. 1939) ("'Real property' includes land and whatever is elected or growing thereon or affixed thereto."); CAL. CIV. CODE § 658 ("Real or immovable property consists of: l. Land; 2. That which is affixed to land; 3. That which is incidental or appurtenant to land; 4. That which is immovable by law; except that for the purposes of sale, emblements, industrial growing crops and things attached to or forming part of the land, which are agreed to be severed before sale or under the contract of sale, shall be treated as goods and be governed by the provisions of the title of this code regulating the sales of goods."); *id.* at § 659 ("Land is the material of the earth, whatever may be the ingredients of which it is composed, whether soil, rock, or other substance, and includes free or occupied space for an indefinite distance upwards as well as downwards, subject to limitations upon the use of airspace imposed, and rights in the use of airspace granted, by law."); *id*. at § 660-662; GER. CIV. CODE § 946 ("if a movable thing is combined with a plot of land in such a way that it becomes an essential part of the plot of land, the ownership of the plot of land extends to this movable thing."); *id*. at § 94 ("The essential parts of a plot of land include the things firmly attached to the land, in particular buildings, and the produce of the plot of land, as long as it is connected with the land. Seed becomes an essential part of the plot of land when it is sown, and a plant when it is planted. The essential parts of a building include the things inserted in order to construct the building."); *see also id.* at §§ 873-902 (providing general provisions on rights in land); *id*. at §§ 925-928 (discussing acquisition and loss of ownership of plots of land).

[57] *See, e. g.*, *City of W. Bend v. Continental IV Fund Ltd. P'ship*, 193 Wis. 2d 481 (Wis. Ct. App. 1995).

obtain the required permits and approvals,[58] and may have to grant access to her neighbors or the public under certain circumstances.[59] And the extraction of water, oil, or minerals is also usually limited where it can affect the environment or the neighboring property owners.[60]

Real property laws grant rights to owners with respect to *physical* manifestations of information that attach to the real property (*e.g.*, warnings carved in stone or a tree, paintings in a cave or on a house, or zebra crossing lines painted on a road), subject to the aforementioned restrictions. The owner of such physical manifestations of information would have the same rights as to the real property itself, including the rights to possess and exclude others from trespassing on the physical embodiment of information (*e.g.*, prohibit others from parking cars on road segments marked with "no parking" lines). But, real property laws do not grant rights to possess or control data about real property.[61] A landowner cannot assert property rights to prohibit others from depicting the location of a zebra road crossing on a map or take a photo of the road markings, or demand access to maps or photos based on ownership of land depicted. Real property ownership does not extend to the informational content, and no ownership rights arise for data as such based on real property laws.

Data is thus not covered by real property laws as protectable subject matter, and real property owners do not have any right to exclude others from accessing, using, reproducing or distributing, the informational content that exists within physical items on their real property.

C. PERSONAL PROPERTY

Personal property laws can grant ownership rights to physical manifestations of information, but do not provide any ownership rights to the underlying information. This is because personal property laws cover

---

58 *See, e.g.*, CAL. GOV. CODE §§ 65000 ff. (2016); STATE OF CALIFORNIA, PLANNING, ZONING, AND DEVELOPMENT LAWS (2012), *available at* http://www.opr.ca.gov/docs/PZD2012.pdf.

59 *See, e.g.*, GER. CIV. CODE § 917(1); Waldgesetz für Bayern [BayWaldG], July 22, 2005, GVBI 313, BayRS 7902-1-L, art. 13(1); *see also* CAL. CIV. CODE § 1009.

60 *See, e.g.*, 30 C.F.R. 250.

61 To the contrary, California law grants a “right of entry” on property to collect information about borders and location of real property. See, Cal. Bus. & Prof. Code § 8774.

physical things (other than real estate). For example, the German Civil Code expressly limits personal property law[62] to tangible things.[63] California property law defines personal property as "every kind of property that is not real [property]"[64] and courts have required a connection to *physical* items.[65] An owner of a physical item that embodies information—such as a book, photo, or computer chip—can thus enforce property rights to the physical item that embodies data (*e.g.*, exclude others from taking a computer chip or demand return of a book),[66] but cannot exclude others from apprehending, using, reproducing, disclosing, or displaying the information contained within the physical item (*i.e.*, informational content).

D. TRADE SECRET

At first sight, trade secret laws may appear to come close to granting ownership rights to data, but these laws have limitations that prevent them from effectively granting property rights to data. In the U.S., trade secret law originated from the common law, but has now been codified in state statutes[67] that resemble the Uniform Trade Secrets Act[68] and Federal law,

---

62 *See* GER. CIV. CODE §§ 929-984 (referring to "movable things").

63 *See* GER. CIV. CODE § 90 ("[O]nly corporeal objects are things as defined by law.").

64 *See* CAL. CIV. CODE § 663.

65 *See Bogan v. Wiley*, 90 Cal. App. 2d 288, 293 (Cal. Ct. App. 1949) (stating that the phrase "property of a decedent" in its restricted meaning is limited to tangible property); 13 WITKIN LIBRARY, *Personal Property*, *in* SUMMARY OF CALIFORNIA LAW § 4 (11th ed. 2017); IMOGEN GOOLD, KATE GREASLE, JONATHAN HERRING & LOANE SKENE, PERSONS, PARTS AND PROPERTY 91 (2014) ("All clear property rights, in addition to being exigible against the world, have a second characteristic of relating to a physical thing.").

66 Lars S. Smith, *Symposium Review: RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695, 737-738 (2006) ("Even if the manufacturer does not own the data directly - whether because the data is not subject to ownership by anyone, or because the manufacturer is not the creator of the data or otherwise directly owner of the intangible property - the manufacturer may be able to control the data because it owns the chip in the tag. Given that the chip (and the antenna) is a piece of tangible, personal property, traditional rules regarding ownership of the chip would apply.")

67 Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 6 (2007).

68 *See* Lars S. Smith, *Symposium Review: RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695, 722 (2006).

including the Defend Trade Secrets Act of 2016.[69] Businesses can claim protection for technical know-how, customer lists, and other information as trade secrets if that information (1) is not generally known or readily accessible, (2) derives an economic value from being secret, and (3) has been subject to reasonable steps to be kept as a secret.[70]

Whether such protection falls within the property law regime is subject to controversy.[71] In the Defend Trade Secrets Act of 2016, Congress expressly stated that the Act "shall not be construed to be a law pertaining to intellectual property."[72] Trade secrets are protected against misappropriation by way of espionage or breach of contract.[73] The goal of trade secret law is not to incentivize citizens or companies to keep information secret, but to protect business integrity from unfair misappropriation of valuable confidential information.[74] In Germany, trade secret protection has also historically been cast as a prohibition

---

[69] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016); codified mostly in 18 U.S.C. § 1836; *Lothar Determann, Luisa Schmaus & Jonathan Tam*, Trade Secret Protection Measures and New Harmonized Laws, 17 Computer L. Rev. Int'l, 2016, 179.

[70] *See* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 25 (6th ed. 2012) ("The definition of subject matter eligible for protection is quite broad: business or technical information of any sort. To benefit from trade secret protection, the information must be a secret."); *see also* 18 U.S.C. §§ 1832, 1839(3)(A)(B); CAL. CIV. CODE §§ 3426.1(d) & 3426.11; Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, art. 2(1), 2016 O.J. (L 157) 1, 9 (laying down corresponding rules for protection to be provided by the EU Member States).

[71] *See, e.g.*, Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 15 (2007) ("To many, if trade secrets are property, then laws protecting them are normatively justified. Thus, the question of whether or not trade secrets are property has raged on for many years.")

[72] Defend Trade Secrets Act § 2(g) is apparently inteded primarily to maintain the status quo under Section 230 Communications Decency Act, see Eric Goldman, The Defend Trade Secrets Act Isn't an 'Intellectual Property' Law, 33 Santa Clara High Tech Law Journal, 541-551 (2017), SSRN: https://ssrn.com/abstract=2924827.

[73] *See* 18 U.S.C. §§ 1832 and 1839(6)(A); CAL. CIV. CODE §§ 3426.1-3426.11.

[74] *See* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 25 (6th ed. 2012) ("Trade secret laws are state law doctrines that protect against the misappropriation of certain confidential information."); *id.* at 37 ("On eligible subject matter, the current trend, exemplified once again by the UTSA, is to protect as a trade secret *any* valuable information so long as the information is capable of adding economic value").

against unfair competition, and not as a property right.[75] Further, trade secrets do not provide "exclusive" rights,[76] and the legal protections available for trade secrets are less concrete than those for real, personal, and other intangible properties.[77] For example, information immediately loses protection under trade secret laws if it becomes public via independent discovery or reverse engineering[78] in the interest of innovation[79]—in other words, the moment the information no longer qualifies as a secret.[80] Trade secret laws are thus more akin to traditional tort law than to property law (*e.g.*, patent or copyright law).[81]

---

75 *See* Gesetz gegen den unlauteren Wettbewerb [UWG] [Act Against Unfair Competition], Mar. 3, 2010, BGBl. I at 254, amended Feb. 17, 2016, BGBl. I at 233 (Ger.), translated in Bundesministerium der Justiz and fur Verbraucherschutz, https://www.gesetze-im-internet.de/englisch_uwg/index.html (last visited Feb. 11, 2018).

76 1-2 MILGRIM ON TRADE SECRETS § 2.01.

77 See Pamela Samuelson, Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?, 38 CATH. U. L. REV. 365, 400 (1989).

78 18 U.S.C. § 1839(6)(B); *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) (defining "reverse engineering" as "starting with the known product and working backward to divine the process which aided in its development or manufacture."); *see also* Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, recital 16, 2016 O.J. (L 157) 1, 4 ("In the interest of innovation and to foster competition, the provisions of the Directive should not create any exclusive right to know-how or information protected as trade secrets. Thus, the independent discovery of the same know-how or information should remain possible. Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed."); *see also* Lothar Determann, Luisa Schmaus & Jonathan Tam, *Trade Secret Protection Measures and New Harmonized Laws*, 17 COMPUTER L. REV. INT'L 179 (2016).

79 *See* Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, recital 16, 2016 O.J. (L 157) 1, 4.

80 The qualification of trade secrets as property is controversial and determined differently for purposes of different areas of law. For example, the U.S. Supreme Court has recognized that if state law recognizes a trade secret as property, then for purposes of a federal "taking" analysis, it is property. 1-2 MILGRIM ON TRADE SECRETS § 2.01.

81 ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 25 (6th ed. 2012); *see also id.* at 37 ("Legal protection for trade secrets is premised primarily on two theories that are only partly complementary. The first is utilitarian. Under this view, protecting against the theft of proprietary information encourages investment in such information. . . The second theory

The limitations of trade secret laws as a means to establish property-like rights in data are particularly evident with respect to data generated by connected cars and other devices on the Internet of Things. Device manufacturers typically cannot access information from devices without the device owners' consent,[82] much less keep the information secret from the device owners. Device manufacturers thus generally cannot claim trade secret ownership rights in the data and information generated by the devices they sell to customers. And consumers also usually cannot claim trade secret rights in the data produced by the devices they own, because they cannot substantiate a competitive advantage from keeping the data secret. Moreover, much of the data and information generated by cars and other connected devices, such as the location and environment, is generated and displayed in plain sight, depriving that information of secrecy. Thus, trade secret laws do not convey meaningful ownership in data, and instead, merely offer some level of protection against unfair misappropriation of information.

E. PATENT

Patent law provides property rights to systems or methods that involve inventive use, storage, or application of data in certain instances. But patent law does not provide any ownership rights in the underlying data itself.

Inventors can acquire patent rights to new, non-obvious and useful processes, machines, manufactures or compositions of matter, and to new and useful improvements thereof.[83] Although the protection granted under patent law is generally broad, and as often cited, embraces "anything under the sun that is made by man,"[84] the U.S. Supreme Court recognizes limitations to patent-eligible subject matter, such as laws of nature, natural phenomena, and abstract ideas.[85] These limitations were described as "the

---

emphasizes deterrence of wrongful acts and is therefore sometimes described as a tort theory.")

82 The U.S. Computer Fraud and Abuse Act and other jurisdictions' computer interference laws expressly prohibit such access. *See* Lothar Determann, *Internet Freedom and Computer Abuse*, 35 HASTINGS COMM. & ENT. L. J. 429 (2013).

83 *See* 35 U.S.C. §§ 101 (utility), 102 (novelty), 103 (nonobviousness).

84 *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980).

85 *Diamond v. Diehr*, 450 U.S. 175, 185 (1981) (citing *Parker v. Flook*, 437 U.S. 584 (1978); *Gottschalk v. Benson*, 409 U.S. 67 (1972); *Funk Bros. Seed Co. v. Kalo*

basic tools of scientific and technological work," for which a monopoly through patent rights would impede innovation.[86] Although use, storage, or application of data can be patentable, the underlying data is not eligible for patent protection.[87] Patent law is thus not an effective legal framework for protecting the rights to data.

F. TRADEMARK

Trademark law also does not provide appropriate property rights to data. Brand names and logos used on goods and services are protected by

---

Inoculant Co., 333 U.S. 127, 130 (1948); *Rubber-Tip Pencil Co. v. Howard*, 87 U.S. 507 (1874)); *see also Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).

[86] ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 145 (6th ed. 2012) (citing *Mayo Collaborative Servs. v. Prometheus Lab., Inc.*, 566 U.S. 66 (2012)).

[87] *Digitech Image Techs. v. Electronics for Imaging*, 758 F.3d 1344 (Fed. Cir. 2014); *see also* W. Nicholson II Price, *Big Data, Patents, and the Future of Medicine*, 37 CARDOZO L. REV. 1401, 1420 (2016) ("Facts and data do not fall within one of the four categories of patentable subject matter. . . This leaves only the algorithms that actually drive black-box medicine as potential subjects of patent protection."). In *Mayo Collaborative Servs. v. Prometheus Labs. Inc.*, 566 U.S. 66 (2012), the Supreme Court illustrated the difference between data and patent-eligible subject matter: The patent in question claimed methods for calibrating the effective dosage for certain drugs to treat autoimmune disease by correlating drug metabolites and the treatment's likely effectiveness. *Id*. The Court held that this data correlation, with little more (telling doctors to increase or decrease the drug based on the metabolite level), was not patentable. *Id.* at 72. The Court referred to the correlation data as a "law of nature" and that "a law of nature is not patentable." *Id.* at 77. The Court explained that one must do something more with the data: apply it in a meaningful way. *Id*. at 71 (explaining that an "*application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.") (emphasis left) (internal quotes removed). But the Court cautioned that "to transform an unpatentable law of nature into a patent-eligible application of such a law, one must do more than simply state the law of nature while adding the words 'apply it.'" *Id*. at 72. The Court provided somewhat more of an explication of what additional application would be sufficient in a later case. *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.* 569 U.S. 576 (2013). There, the PTO granted a patent claiming the isolation of a particular DNA Segment and also the synthetically created DNA (complementary or cDNA). *Id*. The Court held that the DNA segment was nothing more than the product of nature and not patent eligible. But the synthetic DNA is patent eligible because it "does not present the same obstacles to patentability as naturally occurring, isolated DNA segments." *Id*. at 594. The scientists took the data and made something new. *Id*. (explaining that "the lab technician unquestionably creates something new when [synthetic DNA] is made.").

trademark law against unauthorized use in commerce to the extent that such use could confuse consumers.[88] The scope of trademark law has "remained constant and limited: identification of the manufacturer or sponsor of a good or the provider of a service,"[89] with a fair use defense that "forbids a trademark registrant to appropriate a descriptive term for his exclusive use and so prevent others from accurately describing a characteristic of their goods."[90]

Informational content, such as a person's last name used in a business can therefore be trademarked, referring to the use in a particular branch. However, this does not grant ownership rights in the data or information itself (*i.e.*, name), and only entitles the holder to prevent others from using the name in a confusing way (*e.g.*, within the same business branch the trademark was registered for) in connection with selling similar products or services.

G. COPYRIGHT

Copyright law can provide property rights to original works of authorship that contain information, including creative compilations of data, but not to the underlying data itself. Although there are different philosophical foundations of copyright law, the predominant philosophical framework undergirding American copyright law is utilitarian:[91] "The immediate effect of our copyright law is to secure a fair return to an 'author's' creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good."[92]

---

88 *See* 15 U.S.C. § 1114(1) (2012); *see also* Gesetz über den Schutz von Marken und sonstigen Kennzeichen [MarkenG] [Act on the Protection of Trade Marks and Other Symbols], Oct. 25, 1994, BGBl I at 3082, amended Mar. 20, 1996, BGBl I at 3830, § 4 (Ger.) (hereinafter German Trademarks Act).

89 *New Kids on the Block v. News Am. Publ'g, Inc.*, 971 F.2d 302, 305 (9th Cir. 1992).

90 *New Kids on the Block*, 971 F.2d at 306 (citing *Soweco, Inc. v. Shell Oil Co.*, 617 F.2d 1178, 1185 (5th Cir. 1980)).

91 ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 436 (6th ed. 2012); *see also* U.S. CONST. art. I, §8, cl. 8 (granting Congress the power to enact copyright laws in order to "promote the Progress of Science and useful arts.").

92 *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

Authors of writings and other works are thus granted protection under copyright law if they are creative.[93] The subject matter protectable by copyright spans a broad range of literary and artistic expression, including literature, song, dance, sculpture, graphics, painting, photography, sound, movies, and programming code.[94] But copyright law protects only the creative expression of information and not the information itself.[95] Copyright owners hold the exclusive right to exclude others from copying, adapting, distributing, performing, or displaying creative content,[96] but not with respect to the underlying factual information contained within; for example, an accounting book author would be able to assert her rights under copyright law against literal copying of the book's text, but not against differently-worded descriptions of the accounting methods contained within the book.[97] As the U.S. Supreme Court pointed out, in "considering the general question of property in news matter, it is necessary to recognize its dual character, distinguishing between the

---

93 *See* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 429 (6th ed. 2012) (stating that copyright law is "a principal means for protecting works of authorship."); 17 U.S.C. § 102(a); URHEBERRECHTSGESETZ [URHG] [ACT ON COPYRIGHT AND RELATED RIGHTS], Sept. 9, 1965, § 2, BGBL. I at 1273, amended Dec. 20, 2016, BGBL. I at 3037 (Ger.), translated in GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018).

94 ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 434 (6th ed. 2012).

95 *See* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 434 (6th ed. 2012) ("Ideas themselves are not copyrightable, but the author's particular expression of an idea is protectable."); *see also* 17 U.S.C. § 102(b) (2012) ("In no case does copyright protection … extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery."); *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 347–48 (1991) (holding that "all facts – scientific, historical, biographical, and news of the day" are part of the public domain and are not copyrightable). This also true under German copyright law, which requires a certain level of creativity ("Schoepfungshoehe"). *See* URHEBERRECHTSGESETZ [URHG] [ACT ON COPYRIGHT AND RELATED RIGHTS], Sept. 9, 1965, § 2(2), BGBL. I at 1273, amended Dec. 20, 2016, BGBL. I at 3037 (Ger.), translated in GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018).

96 *See* 17 U.S.C. § 106 (2012); URHEBERRECHTSGESETZ [URHG] [ACT ON COPYRIGHT AND RELATED RIGHTS], Sept. 9, 1965, §§ 15-23, BGBL. I at 1273, amended Dec. 20, 2016, BGBL. I at 3037 (Ger.), translated in GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018) (stating that the owner has exclusive right to the relevant actions).

97 *Baker v. Selden*, 101 U.S. 99 (1879).

substance of the information and the particular form or collocation of words in which the writer has communicated it."[98]

In certain instances, copyright law grants copyright ownership rights to compilations of data, as long as that compilation is creative. An author can creatively select or arrange the facts in a compilation, *e.g.*, by choosing which facts to include, in what order to place them and how to arrange the collected data.[99] The resulting compilation then entails a degree of creativity and may therefore possess the requisite originality for copyright protection.[100] But even in such cases, no copyright is attached to the factual data itself.[101]

Where cars and other connected devices generate and record data, the resulting compilations will often already lack human creativity so that an abstraction filtration test to separate facts and creative expression is not even necessary. Neither monkeys taking selfies nor autonomous cars recording security footage can create copyrightable works or own copyrights.[102] When companies write software code to cause connected

---

98 *See International News Service v. Associated Press*, 248 U.S. 215 (1918). Further, various limitations also apply to copyrightable subject matter in the interest of promoting constructive criticisms, comments, news reporting, teaching, scholarship and research. *See* 17 U.S.C. § 107 (2012) (discussing the fair use doctrine); GER. CIV. CODE §§ 903-1011; URHEBERRECHTSGESETZ [URHG] [ACT ON COPYRIGHT AND RELATED RIGHTS], Sept. 9, 1965, §§ 49 & 52a, BGBL. I at 1273, amended Dec. 20, 2016, BGBL. I at 3037 (Ger.), translated in GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018); *see also* Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, OFFICIAL J. L 167 art. 14 (2001) ("This Directive should seek to promote learning and culture by protecting works and other subject-matter while permitting exceptions or limitations in the public interest for the purpose of education and teaching.").

99 *Feist Publ'ns, Inc.*, 499 U.S. at 348.

100 *Feist Publ'ns, Inc.*, 499 U.S. at 363 (declining the copyrightability of the arrangement of data in an telephone directory because there was "nothing remotely creative about arranging names alphabetically in a white pages directory" as this was "an age-old practice, firmly rooted in tradition and so commonplace that it has come to be expected as a matter of course"). This principle is embodied in 17 U.S.C. § 101, which defines "compilation" as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."

101 *See* 17 U.S.C. § 103(a)-(b) (2012).

102 . See, U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES §§306, 313.2 (3d ed. 2017); available at www.copyright.gov/comp3/.

cars or other devices to generate and compile data, human creativity can manifest itself separately and apart from the compiled data, *e.g.*, in the coding of self-learning programs that create maps using artificial intelligence in autonomous cars. It can then be difficult to separate the creative aspects of the resulting work or compilation from the non-protectable factual information.[103] For example, a creator of a database containing information on traffic conditions, road hazards and speed cameras may attempt to claim copyright protection for the compilation.[104] But the database creator will typically be unable to show that the arrangement of the information has any originality.[105]

Further, any protection granted to compilations would in practice only safeguard against a very limited scope of actions. Copyright law again does not extend to the facts contained in the compilation and is limited to the facts' particular selection or arrangement. This means that a subsequent compiler will be free to use the facts contained in the prior compilation, as long as the competing work does not feature the same selection and arrangement.[106] To be successful with copyright claims, a plaintiff thus has to prove that the defendant copied more than the merely-extracted factual information.[107] If a developer reproduces and adapts copyrighted code for the sole purpose of extracting non-copyrightable data from expression within a work of authorship, this is permissible under the fair use doctrine.[108]

In summary, copyright law does not create ownership rights in the data contained within a compilation or database. To the contrary, copyright law expressly leaves out factual information from copyrightable material, and

---

103 *See* Eric Goldman, *Google Defeats Copyright Lawsuit Over Waze Data*, FORBES, (Dec. 16, 2015) (stating that copyright case law regarding facts and compilations was often confusing).

104 *See PhantomALERT, Inc. v. Google Inc.*, No. 15-cv-03986-JCS, 2015 U.S. Dist. LEXIS 167754 (N.D. Cal. Dec. 14, 2015) (dismissing the plaintiff's complaint alleging that the defendant infringed its copyright by copying "Points of Interest," such as traffic conditions, dangerous road segments, road hazards, and traffic enforcement monitors, from the plaintiff's database containing navigation information).

105 *See PhantomALERT, Inc.*, 2015 U.S. Dist. LEXIS 167754.

106 *See Feist Publ'ns, Inc.*, 499 U.S. at 349; 17 U.S.C. § 103(b).

107 *See PhantomALERT, Inc.*, 2016 U.S. Dist. LEXIS 30321, at *17-18 (holding that facts are not original and not copyrightable).

108 . Lothar Determann & David Nimmer, *Software Copyright's Oracle from the Cloud*, 30 BERKELEY TECH. L.J. 161, 175 (2015)

in the U.S., precludes the states from creating copyright-like property regimes for information or data.[109]

H. U.S. STATE LAWS ON MISAPPROPRIATION AND EU DATABASE DIRECTIVE

Companies that invest significant time and effort into the creation of databases can claim limited protection against free-riders under the European database laws[110] and U.S. state laws on misappropriation.[111]

Unlike copyright law, which protects the creativity or authorship arising from a collection of facts, U.S. state laws on misappropriation and European database laws afford limited *sui generis* protection for collections of information that require *significant investments.*[112] These protections are intended and framed as torts to safeguard business integrity

---

109 Unlike the data generated by a device, the software used in connected cars and other devices is protected by copyright law. In the U.S., source and object code of software is protected as "literary work" and thus enjoys the same protections and limitations as copies of other copyrightable works. *See* 17 U.S.C. § 101. Europe grants protection to software copies in the EU Software Directive 2009/24/EC. *See* Directive 2009/24/EC of the European Parliament and of the Council of April 23, 2009 on the Legal Protection of Computer Programs, 2009 O.J. (L 111) 16. For a detailed discussion, see Lothar Determann & David Nimmer, *Software Copyright's Oracle from the Cloud*, 30 BERKELEY TECH. L.J. 161, 165-172 (2015) and Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329, 1354 (1987). For an overview of software copyright protection in the EU, see Pamela Samuelson, *Comparing U.S. and EC Copyright Protection for Computer Programs: Are They More Different Than They Seem?*, 13 J.L. & COM. 279 (1994).

110 *See* Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) (hereinafter EC Database Directive) (offering copyright-like protection to creators of valuable databases).

111 *See, e.g.*, *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 852-54 (2d Cir. 1997) (discussing the merits of a "hot news" misappropriation claim in the context of unauthorized electronic delivery of near-real-time professional basketball statistics); *United States Golf Ass'n v. Arroyo Software Corp.*, 69 Cal. App. 4th 607, 611-12 & 618 (1999) (discussing California's common law misappropriation as applicable to the unauthorized use of golf handicap formulas that were developed through intensive data collection and analysis); *Bd. of Trade City of Chicago v. Dow Jones and Co.*, 439 N.E.2d 526, 537 (Ill. App. Ct. 1982) (applying Illinois' common law misappropriation to the unauthorized use of the Dow Jones Index and Averages as a trading vehicle); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (1995); Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Data-Bases in the United States and Abroad*, 66 U. CIN. L. REV. 151, 157 et seq. (1997).

112 Art. 7 of Directive 96/9/EC on the legal protection of data bases, OJ 1996, L 77/20; *see generally* Lothar Determann, Luisa Schmaus & Jonathan Tam, *Trade Secret Protection Measures and New Harmonized Laws*, 17 COMPUTER L. REV. INT'L 179 (2016).

and fair competition.[113] For the same reasons, news organizations can claim limited protection for "hot news items" against immediate copying by free-riders only if the factual information is time-sensitive and requires significant efforts to discover.[114] But such limited protections against freeriding by competitors are not framed as property law regimes and, like trade secret laws, constitute only narrow exceptions to the general rule that facts should be generally accessible and not subject to individual exclusivity rights.

In the EU, the financial and professional investment in an arrangement of facts is safeguarded through a *sui generis* right to enable database makers[115] to protect their respective time, money, and effort;[116] they are entitled to prevent extraction or re-utilization of the whole or a substantial part (qualitatively or quantitatively) of the database.[117] But, full copyright-like property protections in European database protection laws apply only

---

113 Rectials 6 and 7 of Directive 96/9/EC on the legal protection of data bases, OJ 1996, L 77/20 explain the legislative considerations and intent as follows: "copyright remains an appropriate form of exclusive right for authors who have created databases; (...) nevertheless, in the absence of a harmonized system of unfair-competition legislation or of case-law, other measures are required in addition to prevent the unauthorized extraction and/or reutilization of the contents of a database..."

114 See International News Service v. Associated Press, 248 U.S. 215 (1918).

115 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77), at art 1(2) (defining the term "database" as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.")

116 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77), at ¶¶ 39-40 ("[T]his Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor, . . . the object of this sui generis right is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right; whereas such investment may consist in the deployment of financial resources and/or the expending of time, effort and energy.")

117 *See* Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77), at art 7(1); *see also* URHEBERRECHTSGESETZ [URHG] [ACT ON COPYRIGHT AND RELATED RIGHTS], Sept. 9, 1965, § 97 BGBL. I at 1273, amended Dec. 20, 2016, BGBL. I at 3037 (Ger.), translated in GESETZE IM INTERNET, https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (last visited Jan. 23, 2018) (stating a right to require cessation of infringement and to damages).

to the creative selection or arrangement of the factual information, which carves out the individual information elements from ownership.[118]

If a device manufacturer, software company or online service provider deliberately configures a connected device to collect and report the data for purposes of creating a database—and obtains the required consents and authorizations from the device buyers to legally create such a database—then the company may acquire limited ownership rights in that database under U.S. state laws on commercial misappropriation and EU database protection laws.[119] Also, companies can develop, purchase, deploy and configure connected devices specifically to create a database that is valuable to their business and then claim database protection rights, *e.g.*, a weather forecast company that deploys drones and sensors to collect up-to-date weather information or a traffic advisory service provider that guides drivers to find the quickest routes.

But in the absence of deliberate database creation plans and investments, neither the EU database directive nor the U.S. state laws on misappropriation offers significant property rights with respect to data generated by connected cars or other devices as mere byproducts.[120] Even when limited exclusivity rights do attach, available remedies have limited scopes: protection is only applicable against wholesale copying of the database or substantial parts of it, typically where freeriding could have a noticeable impact on investments and competition. Individual information

---

118 See also Malte Gruetzmacher, Dateneigentum – ein Flickenteppich, Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, C.R. 485, 488 (2016) (Ger.).

119 CJEU, C-203/02, ECLI:EU:C:2004:695 #42 – The British Horseracing Board Ltd; Rs. C-444/02, ECLI:EU:C:2004:697 #4 – Fixtures Marketing Ltd.; BGH, GRUR 2010, 1004 (1005); Salestraq Am., LLC v. Zyskowski, 635 F. Supp. 2d 1178, 1185 (D. Nev. 2009); Opperman v. Path, Inc., 84 F. Supp. 3d 962, 972 (N.D. Cal. 2015); but see, Firoozye v. Earthlink Network, 153 F. Supp. 2d 1115, 1131 (N.D. Cal. 2001);

120 See Malte Gruetzmacher, Dateneigentum – ein Flickenteppich, Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, C.R. 485, 487-488 (2016) (Ger.); Thomas J. Farkas, Data Created by the Internet of Things: The New Gold without Ownership, 23 REV. PROP. INMATERIAL 5, 9 (2017) ("[I]n case of the networked car, the data generated by virtue of the sensors must rather be regarded as raw data. E.g., the data regarding location and driving behaviour is rather not in a systematic or methodical order."); see also Josef Drexl et al., Data Ownership and Access To Data, MAX PLANCK INST. FOR INNOVATION & COMPETITION 1, 10 (2016), available at https://papers.ssrn.com/abstract=2833165. For a discussion on how information generated from the collected data might be granted protection, see Lothar Determann, Social Media Privacy: A Dozen Myths and Facts, STAN. TECH L. REV. 7, 3 (2012).

content elements, however, are excluded from protection under database protection laws in the interest of protecting public interests in information.

I. DATA PRIVACY

Data privacy laws are intended to protect individual freedom and human dignity.[121] They favor data minimization and are not intended to incentivize creation or production. Privacy laws are thus generally not referred to as property laws.[122]

Privacy laws give data subjects the right to exclude others from acquiring or using certain personal information about them, similarly to the exclusion rights conferred by property laws.[123] EU lawmakers have taken broad action to protect data privacy and have restated in the new General Data Protection Regulation (GDPR) that companies are generally prohibited from processing any personal data unless there is a statutory exception.[124] Such strongly worded exclusion rights have been likened to property law concepts.[125] Yet, GDPR stops short of recognizing ownership or property rights for data subjects and refers to "ownership" and "property" only to recognize the conflicting rights that may outweigh

---

121 *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) ¶1, 2016 O.J. (L 119) 1, 1.

122 Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2059 (2004).

123 Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130 (2000).

124 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6, 2016 O.J. (L 119) 1, 36 (defining "personal data" as "any information relating to an identified or identifiable natural person"); *id*. at art. 4(2) (defining "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction").

125 *See, e.g.*, Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L. J. 513, 515 (2013) ("Regulation takes the unprecedented step of, in effect, creating a property regime in personal data."); Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2059 (2004).

privacy interests.[126] Even the novel right to data portability is quite limited: it applies only to personal data provided (not: created or acquired by an "owner"), by the data subject (not: any "owner"), based on consent or contract (not: legitimate interests, law or other bases), and does not confer any exclusion, usage or alienation rights.[127]

In the U.S., overlapping federal and state regulations on data privacy[128] protect reasonable privacy expectations under tort laws and sector-specific regulations with even less of a property law-like character as provided in GDPR.[129]

For instance, the Health Insurance Portability and Accountability Act (HIPAA), which is the federal statute governing healthcare data, protects the privacy of individually identifiable information, but does not grant any ownership rights to the individuals in their records.[130] For a few state statutes pertaining to automotive event data recorders (EDRs), which serve as "black boxes" for recording critical sensor and diagnostic data prior to collisions, legislatures have used a property law terminology and allocated "ownership" to data from EDRs to drivers or vehicle owners.[131] But the statutes make clear that their intent is to allocate ownership to the physical embodiment of data on the tangible EDR devices, and not to create property rights to the information content itself, which eye witnesses, security cameras, other traffic participants and forensic investigators are free to acquire from other sources. Similarly, California privacy laws impose security breach notification obligations on "owners" of certain

---

126 *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) ¶63, 2016 O.J. (L 119) 1, 12.

127 See, Art. 20 GDPR.

128 Erika G. Martin & Grace M. Begany, *Opening Government Health Data to the Public: Benefits, Challenges, and Lessons Learned from Early Innovators*, 24 J. OF THE AM. MED. INFORMATICS ASS'N 345, 348 (2017), *available at* https://academic.oup.com/jamia/article/24/2/345/2631468.

129 Lothar Determann, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW (3d ed. 2017), p. xvii et seq.

130 HEALTH INFO. & THE LAW, WHO OWNS HEALTH INFORMATION? 1 (2015), http://www.healthinfolaw.org/lb/download-document/6640/field_article_file.

131 *See, e.g.*, ARK. CODE. § 23-112-107(c),(e) (2010); ORE. REV. STAT. § 105.928; *see also* Frederick J. Pomerantz & Aaron J. Aisen, *Auto Insurance Telematics - Data Privacy And Ownership*, 20-11 MEALEY'S EMERG. INS. DISPS. 13 (2015).

computerized data,[132] but clarify in their definitional section that the "ownership" term is broadly deployed to protect any data held by a company for its own business purposes[133] (as opposed to data handled by a service provider, which are subject to different notification rules).[134] Thus, even though the California legislature uses the term "owner" in connection with "data," it neither relies on existing property law concepts nor recognizes property rights to data.

In the California Consumer Privacy Act, which was enacted in June 2018 and becomes effective in January 2020, California imposes significant restrictions on sales of personal information: Consumers receive far-reaching rights to demand data access, erasure and portability, and to prohibit sales of their data.[135] Businesses must not charge or penalize consumers for exercising their rights. Consequently, companies find the value of personal information and their options with respect to the use, sharing and monetization of data greatly reduced. Thus, California protects individual privacy from alleged risks associated with data sharing and commercialization with a legal regime that inhibits trade in personal information. By creating inalienable[136] opt-out, erasure and portability rights in personal information, the California Consumer Privacy Act significantly limits the level of control that businesses can acquire or retain over personal information. As a result, the law also reduces the potential profit for consumers from selling personal information, because

---

132 CAL. CIV. CODE § 1798.82(a).

133 *See* CAL. CIV. CODE §1798.81.5(a) ("(1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information. (2) For the purpose of this section, the terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.")

134 Lothar Determann, CALIFORNIA PRIVACY LAW - PRACTICAL GUIDE AND COMMENTARY, Ch. 2-15.1 (3d ed. 2018, forthcoming).

135 Lothar Determann, New California Privacy Law Against Data Trade - the California Consumer Privacy Act of 2018, broad data and business regulation, applicable worldwide, Computer & Internet Lawyer (forthcoming 2018); The California Consumer Privacy Act, IAPP Advisor July 2, 2018.

136 Cal. Civil Code §1798.192.

it renders consumers legally incapable of effectively waiving rights to data access, erasure, porting or right to prohibit data sharing. Thus, the California Consumer Privacy Act goes into the opposite direction of creating property rights to data and further diminishes any potential for commercial interests in personal information.

Legal scholars, on the other hand, have proposed information property law regimes to protect privacy.[137] Data protection authorities in the EU also encourage the thought that individual persons own the personal data relating to them,[138] and popular rhetoric regarding privacy protections gives people elsewhere the idea that they "own" their personal data.[139] Yet, except for exclusion rights, data protection and privacy laws diverge from property laws. Privacy laws do not incentivize or reward creation or investment, do not regulate the acquisition or transfer of ownership rights to others, and do not apply against everyone. Instead, EU data protection laws confer exclusion rights against governments and businesses, but not against individuals acting for personal or household purposes;[140] most U.S. data privacy laws tend to be sector-specific and apply to certain types of businesses, organizations or individuals,[141] unlike property laws, which tend to apply to everyone.[142]

---

137 *See, e.g.*, Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004); Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 247 (2002).

138 *See, e.g.*, UK INFORMATION COMMISSIONER'S OFFICE (ICO), *ICO Warns Data Broking Industry After Issuing £80,000 Fine to Unlawful Data Supplier* (Nov. 2, 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/ico-warns-data-broking-industry-after-issuing-80-000-fine-to-unlawful-data-supplier/ (stating that an ICO representative's statement that "Businesses need to understand they don't own personal data - people do.").

139 *Cf.* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130 (2000) (discussing and refuting the possible reasons why individuals might naturally assume they own data about themselves); *see also* Thomas de Maizière, DER TAGESSPIEGEL (Feb. 16, 2017), http://www.tagesspiegel.de/politik/data-debates-datenschutz-ist-kein-selbstzweck/19391956.html (stating that the people's assumption of data ownership is mistaken).

140 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 2(2)(c), 2016 O.J. (L 119) 1, 32.

141 *See* Lothar Determann, California Privacy Law - Practical Guide and Commentary (3d ed. 2018, forthcoming).

142 *See, e.g.*, Herbert Zech, Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers, C.R. 137, 139 (2015) (Ger.).

J. SUMMARY

Real and personal property laws may protect physical embodiments of information, including data on storage disks within computers, stationary server farms, or event data recorders (aka "black boxes") in cars, or as warning signs on walls or roads, but such protection does not extend to the informational content. Intellectual property laws (notably in copyright and patent laws) tend to carve out factual content from protected subject matter to preserve public access to such factual information. Creative information collection schemes and valuable databases that are subject to significant investments enjoy some limited protection against copying and freeriding, but individual information elements are still not protected. Trade secret law can protect factual information, but only if the information is kept secret and provides economic value from being a secret. U.S. data privacy and EU data protection laws do not greatly resemble property law regimes, but afford important exclusion rights to data subjects, which are further examined in Parts IV and V. Thus, the answer to the question "*who owns the data generated from connected cars and other Internet of Things devices?"* is "*no one, really*."

IV. DATA ACCESS RIGHTS AND RESTRICTIONS UNDER CURRENT LAW

No one owns property rights in data, as shown in Part III, but the complex landscape of data access rights and restrictions, summarized in this Part IV, created by legislatures and courts for various purposes and interests, summarized in Part V, serves as a basis for a discussion in Part VI of this Article, which addresses whether additional property rights in data are needed, helpful or harmful.

A. RIGHTS TO DATA ACCESS, ERASURE, PORTABILITY AND USE RESTRICTIONS

Data subjects (*e.g.*, drivers, patients, cellphone owners) do not generally own data about them,[143] but are entitled to certain restrictions regarding the use of their data by companies and governments under data

143 As mentioned, restrictions from data privacy do just not lead to property rights. *See supra* Part III.I; Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, STAN. TECH L. REV. 7, 3 (2012).

privacy laws.[144] And they are further entitled to access, erasure, and portability of their personal data processed by companies under data protection laws in the EU and other jurisdictions.[145]

B. COMPUTER INTERFERENCE LAWS

Owners of data-generating devices (*e.g.*, cars, heart monitors, phones and other connected devices) are protected from access to data and information stored on their devices under computer interference laws such as the U.S. Computer Fraud and Abuse Act (CFAA), which prohibits people from accessing a computer to obtain information without or beyond the scope of authorization.[146] Computer and software manufacturers thus have to obtain authorization from end-users before any error report is sent back or any device is accessed for repair and maintenance purposes. The same applies to manufacturers of connected cars—manufacturers are prohibited from designing cars that automatically send data back to them without authorization from the car owner. Although the car owners will likely provide such authorization in consideration for various services, such as for navigation, traffic updates, accident reports, entertainment, and telematics services, those authorizations will be provided only when something of value is offered by the service providers.

C. RIGHT TO REPAIR STATUTES AND ENVIRONMENTAL AND COMPETITION LAWS

Car manufacturers need to design cars with prescribed degrees of openness under the "right to repair" statutes, environmental laws requiring independent emission tests, and general competition laws.[147] Any device,

---

144 This issue is comprehensively presented in LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW (3d ed. 2017).

145 *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 15, 2016 O.J. (L 119) 1, 43; *id.* at art. 17 (right to erasure); *id.* at art. 20 (right to data portability).

146 18 U.S.C. § 1030 (a)(2)(c). *But see* 18 U.S.C. § 1030 (e)(2) (defining "protected computer" as practically including any ordinary computer and cellphone connected to the internet, as the internet is regarded as an instrumentality of interstate commerce as required by the definition).

147 To protect consumers, lawmakers have proposed or passed various statutes on the "right to repair" doctrine, requiring automakers to provide the same information to independent repair shops as they do to their authorized dealer network. *See, e.g.*, Repair

software, or online service provider that designs technical restrictions on its own products to favor its own spare parts, add-on products, or services can be subject to serious sanctions under antitrust laws, as recently demonstrated by a €2.4 billion fine against an online search provider for offering an internet search service that allegedly favors its own content.[148] Given that device manufacturers naturally have market power for spares and add-on services,[149] their level of discretion on adding restraints on interfaces, ports and other data access means with regard to device owners and spare part providers is limited by these statutes and laws.

D. LAWS ON CONSUMER PROTECTION, PRODUCT SAFETY, IMPLIED WARRANTIES AND SUSTAINABILITY

Consumers are protected against threats posed by connected cars and other devices under product safety, product liability, and contract laws,[150]

Association, http://repair.org/association. The lawmakers are therefore directly focusing on protecting a basic level of openness in cars. *See, e.g.*, On-Board Diagnostic II (OBD II) Systems – Fact Sheet / FAQs, CAL. AIR RES. BD. (Oct. 28, 2015), https://www.arb.ca.gov/msprog/obdprog/obdfaq.htm (showing that California Air Resource Board developed On-Board Diagnostic (OBD) requirements to monitor nearly every component that could affect the emissions performance of a vehicle). Thus, requirements originating from California environmental legislation already establish an important degree of openness. The U.S. Environmental Protection Agency (EPA) along with state agencies such as the California Air Resources Board continue to regulate emission-related parts. *See* EPA Emission Standards Reference Guide for On-road and Nonroad Vehicles and Engines, U.S. ENVTL. PROT. AGENCY, https://www.epa.gov/emission-standards-reference-guide (last visited Jan. 20, 2018). Under antitrust and competition laws, as well as self-regulatory undertakings, car manufacturers cannot monopolize aftermarkets for parts and add-on products.

148 See Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service, EUROPEAN COMMISSION (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

149 So long as several strong car manufacturers remain present on international markets, competition remains sufficiently strong. Monopolization challenges will therefore focus on aftermarket products for a particular brand, arguing that automotive manufacturers have monopoly power in the aftermarket for their own cars and willfully maintain such power through anticompetitive means. *Cf. Eastman Kodak Co. v. Image Tech. Servs.*, 504 U.S. 451, 481 (1992) (citing *United States v. Grinnell Corp.*, 384 U.S. 563, 570–571 (1966)). Some courts have included an explicit third factor that the plaintiff suffer an antitrust injury as a result. *See In re* Independent Serv. Orgs. Antitrust Litig., 114 F. Supp. 2d 1070, 1087 (D. Kan. 2000).

150 *See* 15 U.S.C. § 2056 (2012); 49 U.S.C. § 301 (2012); 49 C.F.R. § 501 (2016); *see also* Request for Public Comments: Safety-Related Defects and Emerging

which require manufacturers, distributors, and add-on service providers to ensure that any of the connected devices and services that they sell are designed to function in a safe and functional manner.[151] Safety considerations warrant interfaces and access means that are sufficiently "open" to allow device owners to update, upgrade, and secure products over time.[152] Depending on how consumer expectations and laws develop around the openness of cars, in the future, a connected car with insufficient interoperability or upgradability may become legally declared as defective under the product safety, product liability, and warranty laws, and run afoul of environmental sustainability requirements, because of its unnecessarily short life cycle.[153]

II. INTERESTS IN DATA AND LEGAL PROTECTIONS UNDER CURRENT LAW

Persons, businesses, and governments have different interests in data. This Part V examines such interests in the context of an entire ecosystem of persons and entities involved with the Internet of Things - instead of selectively citing to anecdotal scenarios and unconnected interests. The interests of parties concerned are identified and associated with existing legal protections available under current law (summarized *supra* in Part IV) to lay the ground work for identifying any potential gaps that could warrant ownership rights in data, which do not yet exist (as discussed in Part III) but are contemplated (as discussed in Part VI). For illustration purposes, this Part V specifically refers to data generated by cars as an

---

Automotive Technologies, 81 Fed. Reg. 18935 (Apr. 1, 2016); *see* Restatement (Third) of Torts: Product Liability §1 (The American Law Institute 1998).

151 The most recent restatement on product liability states that "a product is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe." *See* Restatement (Third) of Torts: Product Liability §2(b) (The American Law Institute 1998).

152 *See* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 1, 16-18 (forthcoming 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837598.

153 *See* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 1, 16-18 (forthcoming 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837598.

example for a data interest landscape that has recently given rise to demands for a data ownership regime by the German government.

A. CAR OWNERS

Most car buyers will be interested in data accessibility, safety features and, interoperability to ensure competitive pricing and availability of data-driven services (*e.g.*, navigation, autonomous driving, and entertainment), spare parts, updates, upgrades, and maintenance services.[154] Car owners will need open ports in their cars to install brand-agnostics telematics and fleet management technologies, trackers required by insurance companies for individual tariffs, software, and devices to participate in ride-sharing models, and other add-ons, updates, and upgrades.[155] Buyers will pursue their interests primarily by expressing preferences in the marketplace, *e.g.*, buying cars that best meet their needs on data accessibility and interoperability. If manufacturers are overly restrictive or not upfront about the technological restraints on data access or interoperability, they may be penalized through complaints that get filed to consumer and competition supervisory bodies.

With respect to data privacy, consumers and business owners will be in slightly different situations. For example, when a consumer owns a car, much of the data generated by the car will qualify as "personal data" because of its relationship with the individual owner; consequently, the consumer will be able to rely on data privacy, consumer protection, and computer interference laws to object to unwanted data access and usage by the manufacturer, distributor, add-on service providers, and others. Business owners on the other hand can take "data privacy by design"

---

154 *See* Simon Ninan, Bharath Gangula, Matthias von Alten & Brenna Sniderman, *Who Owns the Road? The IoT-Connected Car of Today—and Tomorrow*, DELOITTE INSIGHTS (Aug. 2015), https://www.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-automotive-industry.html; *see also* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 1, 17-18 (forthcoming 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837598 (stating that the car might otherwise become unsafe or unusable and be subject to obsolescence).

155 *See* Masa Hasegawa, *Connected Vehicles Enter the Mainstream - Trends and Strategic Implications for the Automotive Industry*, DELOITTE 10 (2012), *available at* https://www2.deloitte.com/us/en/pages/manufacturing/articles/connected-vehicles-enter-the-mainstream.html (stating that vehicle consumers will likely expect their vehicle systems to maintain compatibility with newly purchased consumer electronics for five to six years, the average length of new vehicle ownership in the United States).

measures to sever the relationship between the vehicles and their individual drivers by keeping the individual names out of the telematics systems, but the drivers will be able to rely on computer interference laws to object to unwanted data access by manufacturers and others.[156] Owners of large vehicle fleets (*e.g.*, car rental companies, transportation businesses, ride sharing ventures, logistics providers, and other enterprises) have more pressing needs for brand-agonistic and interoperable data access to optimize fleet management, operation, and maintenance.[157] Such owners will want various information, such as the location of each car, any need for maintenance, differences in fuel consumptions between different vehicle models, whether maximum working hour limits are being followed by the drivers, and ways in which their return on investment can be maximized from the vehicles.

B. DRIVERS AND PASSENGERS

Drivers and passengers will generally be most interested in privacy and safety. Under current law, they are entitled to the provision of notice and choices regarding location-tracking and monitoring by the car owner, manufacturer, or others.[158] Employee drivers can be advised of the employer's data processing activities in accordance with the relevant laws.[159] Car rental customers and taxicab passengers can be reached by pop-up notices in the car to enable their decision-making on whether to permit a certain functionality—*e.g.*, security cameras in the car,

---

156 *See supra* Part IV.B. (referring to 18 U.S.C. § 1030 (a)(2)(c)).

157 *See* James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY 1, 70 (June 2011), *available at* https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

158 *See supra* Parts III.I and IV.A.

159 *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1004–05 (2011) ("Employers can - and often do - destroy any actual expectation of privacy by notifying employees in painstaking detail about the existence and intrusiveness of monitoring and surveillance technologies deployed."). But employers have successfully defended against privacy claims when the tracked vehicles were company-owned, particularly in cases where the tracking was to determine employee misconduct. *See* Karla Grossenbacher, *Employee GPS Tracking - Is It Legal?*, LEXOLOGY: THE GLOBAL PRIVACY WATCH BLOG (Jan. 26, 2016), http://www.lexology.com/library/detail.aspx?g=a94fd053-3106-4836-bc9c-a25d05340ed5.

entertainment solutions, navigation systems, or location tracking—or to refrain from using a particular vehicle if not configurable.

C. OTHER TRAFFIC PARTICIPANTS

Connected cars will communicate with other traffic participants, including other cars and their drivers, as well as cyclists, pedestrians, and bystanders, for safety reasons.[160] Opportunities for providing proper notice and giving choices on data access will be limited, however, and standardization through legislation may thus be required. In the meantime, car manufacturers and owners will need to ensure that connected cars are constructed with "data privacy by design" principles in mind, so that there will be no illegal data collection or usage.[161]

D. MANUFACTURERS

Manufacturers can use data generated from connected cars to monitor maintenance status; anticipate and prevent failures; improve products;

---

160 *See* EU Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, Brussels 30.11.2016, COM(2016) 766 final.

161 Pushing for "privacy by design" requirements, the U.S. FTC has brought a number of cases against product manufacturers that did not sufficiently consider data security in the design of their products, which have included network cameras, home routers, and software platforms. *See, e.g.*, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, FED. TRADE COMM'N (Sept. 4, 2014), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles; F*ed. Trade Comm'n, ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk*, FED. TRADE COMM'N (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put/; *Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates*, FED. TRADE COMM'N (Dec. 21, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java). Under the GDPR, companies will be expressly required to consider data protection by design and by default and implement appropriate technical and organizational measures. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 25, 2016 O.J. (L 119) 1, 48. For a discussion on technical principles and implementation of IT security regarding the mentioned communications see Thomas Strubbe, Nicolas Thenee & Christian Wieschebrink, *IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen*, DATENSCHUTZ UND DATENSICHERHEIT 223, 223 (2013) (Ger.).

develop new products and/or offer add-on services, updates, and upgrades.[162] These manufacturers' interests will be largely aligned with the interests of car owners so long as the manufacturers do not use the data against the interests of the car owners (*e.g.*, by selling information on speeding violations to law enforcement agencies);[163] car owners will then remain informed about the manufacturers' use of the car owners' data, and data access ports will remain open enough to allow the car owners to choose alternatives to the manufacturers' offered updates, upgrades, and add-on services.[164]

Manufacturers will not be legally entitled to receive any data from their sold cars, but they may design the cars in ways that automatically report the collected data back to their makers, as long as they obtain authorization from car owners (as required under computer interference laws)[165] and provide sufficient notice and choices to car owners, drivers, passengers, and others regarding any personal data collected by the car manufacturers.[166]

Manufacturers will also have interests in restraining access to technical data, primarily for three reasons: to (1) guard trade secrets on their manufacturing processes and technologies installed in the cars; (2) reduce

---

162 See Thilo Weichert, Datenschutz im Auto - Teil 1, das Kfz als grosses Smartphone mit Raedern, SVR 201, 202 (2014) (Ger.); see also David Welch, Your Car Has Been Studying You; Everyone Wants the Data, BLOOMBERG TECH. (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/your-car-s-been-studying-you-closely-and-everyone-wants-the-data.

163 This example may seem farfetched at first glance, but some concerns have surfaced regarding sharing of navigation system information with government agencies. *See* Archibald Preuschat, *TomTom Drives Into Speed Camera Scandal*, THE WALL STREET J. (Apr. 28, 2011), http://blogs.wsj.com/tech-europe/2011/04/28/tomtom-drives-into-speed-camera-scandal.

164 *See* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 1, 32 (forthcoming 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837598 (discussing interests in a level of "open interfaces"); Carol Sledge, *A Discussion on Open-Systems Architecture*, SEI BLOG (Nov. 23, 2015), https://insights.sei.cmu.edu/sei_blog/2015/11/a-discussion-on-open-systems-architecture.html)); *Acceleration of the Connected Experience - Vehicle Connectivity and Evolving Customer Expectations*, DELOITTE (2014), https://www.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-automotive-connected-vehicle-100914.pdf (stating that customer expectations evolved as a result of the technical evolution).

165 *See supra* Part IV.B. (referring to 18 U.S.C. § 1030 (a)(2)(c)).

166 *See supra* Part III.I. and IV.A.

potential product liability and reputational harm resulting from aftermarket parts and manipulations, including cybersecurity weaknesses; and (3) reduce competition for spare parts, add-ons, updates, and upgrades in favor of the manufacturer's own offerings. These interests of car manufacturers to restrain data access can come into conflict with competition laws and data access interests of car owners, who may reverse-engineer their products under trade secret law and are generally free to modify and upgrade their products, so long as they comply with the applicable laws.[167] Due to market forces and reverse-engineering possibilities, manufacturers will be incentivized to offer reasonable compromises on data access to buyers. Manufacturers can decide to offer more open (as opposed to closed or locked-in) products at different price-points, similarly to how DVD player manufacturers market region-free players or how mobile phone makers and service providers market unlocked phones and month-to-month contracts.[168]

E. ADD-ON SERVICE PROVIDERS

Add-on or "aftermarket" providers of services, parts, and features will have similar needs and interests as the manufacturers in collecting and processing relevant data.[169] And similar to manufacturers, add-on service providers are not entitled to access any data, except with the authorization from the car owners and when in compliance with applicable data privacy laws.[170] Companies that offer products or services competing with the manufacturer may be entitled to fair and non-discriminatory access to data from the cars under antitrust laws.[171] If a car owner chooses a service, the provider will typically need some data to perform the service (*e.g.*, location data for GPS), in which case the request for an authorization needs to be spelled out in the applicable contract.[172] In turn, the data

---

167 *See supra* Parts III.D. and IV.C.

168 *See, e.g.*, Robert Silva, *What You Need to Know About DVD Region Codes*, LIFEWIRE (June 4, 2017), https://www.lifewire.com/dvd-region-codes-1845720.

169 *See supra* Part V.D.

170 *See supra* Parts III.I, IV.A and IV.B.

171 *See supra* Part IV.C..

172 For discussions on the requirements arising from data privacy laws and computer interference laws, *see supra* Parts III.I, IV.A and IV.B.

generated by the services will also attract the interests of various entities, such as government institutions.[173]

F. CAR DEALERS AND DISTRIBUTORS

Car dealers and distributors of spare parts, add-on products, updates, and upgrades will be interested in information relating to customer-relationship management, so that they can market additional products and services to car owners. Car dealers and distributors are usually permitted to use transaction information to market similar products and services, and they can obtain the customers' consent to direct marketing in connection with the initial sale. For any access to data generated by cars, distributors will need to obtain authorizations from the car owners and possibly provide notice and choices to other data subjects involved, similar to the car manufacturers and add-on service providers,[174] as discussed above.

G. INSURANCE COMPANIES

Insurance companies will be interested in information on driving patterns so that they can assess and reduce risks, for example, through individual tariffs, which reward good driving and punish bad driving.[175] They will need voluntary consent from the car owners for any data access and must comply with the data privacy laws that protect the privacies of drivers, passengers, and others, if and to the extent data is gathered indirectly from them.[176] Where insurance companies offer individual

---

173 Cheryl Miller, *Uber and Lyft Resist Regulators' Appeal for Data Sharing*, THE RECORDER (Oct. 10, 2017) (stating that Uber and Lyft are required by law to submit confidential annual reports to governmental institutions about the types of service they provide, what neighborhoods they serve and how many miles their drivers log) (describing that cities and local transportation planning agencies, however, are eager to get additional information from ride-hailing companies to study traffic patterns and the fast-growing industry's effect on roads and the environment, while the companies refuse sharing this data with public agencies referring to the privacy of both riders and drivers).

174 *See supra* Parts V.D and V.E.

175 Aala S. Reddy, *The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car*, COGNIZANT (Aug. 2012), https://www.cognizant.com/InsightsWhitepapers/The-New-Auto-Insurance-Ecosystem-Telematics-Mobility-and-the-Connected-Car.pdf; *see also* David Welch, *Your Car Has Been Studying You; Everyone Wants the Data*, BLOOMBERG TECH. (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/your-car-s-been-studying-you-closely-and-everyone-wants-the-data; Gerrit Hornung & Thilo Goeble, *"Data Ownership" im Vernetzten Automobil*, C.R. 265, 268 (2015) (Ger.).

176 *See supra* Parts III.I and IV.A.

tariffs as a discount, consumers and regulators can raise the question on whether consent is truly voluntary, given that a policyholder's discount is another policyholder's penalty.[177] A significant penalty for failure to agree to tracking of driving patterns could be deemed as being coercive, depending on the circumstances.[178]

H. LAW ENFORCEMENT AND GOVERNMENT INSTITUTIONS

Law enforcement agencies and civil litigants will be interested in data generated by cars, in connection with accidents and traffic law violations.[179] Under the applicable laws, they will typically need a court order or a voluntary consent from the car owner to access the data stored on a particular car. But they may be permitted to observe cars that are on public roads without limitations, as long as they do not interfere with the physical possession and property rights of the car owner.[180] If manufacturers, service providers, insurance companies, and others have custody of data, law enforcement agencies and civil litigants can try to compel those entities to release the requisite data.[181] This in turn creates a need for those parties to carefully plan and protect their positions.[182]

---

177 See Patrick R. Mueller, Every Time You Brake, Every Turn You Make I'll Be Watching You: Protecting Driver Privacy In Event Data Recorder Information, WIS. L. REV. 135, 158-159 (2006).

178 Cf. Patrick R. Mueller, Every Time You Brake, Every Turn You Make I'll Be Watching You: Protecting Driver Privacy In Event Data Recorder Information, WIS. L. REV. 135, 158-159 (2006).

179 *See* Vince Bond Jr., *Lawyers Reaching for In-Car Data*, AUTOMOTIVE NEWS, (Sept. 14, 2014), http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data.

180 *See United States v. Jones*, 132 S. Ct. 945 (2012) (holding that the government's installation of a GPS device on a target's vehicle and its use of that device to monitor the vehicle's movements is a physical intrusion upon the car, constituting a "search" under the Fourth Amendment).

181 *See supra* Part V.H (discussing the interests of governmental institutions, cities and local transportation planning agencies against ride-hailing companies).

182 *See* Lothar Determann, *Views on Global Surveillance Laws From of Baker & McKenzie*, BLOOMBERG BNA (May 23, 2016), https://www.bna.com/views-global-surveillance-n57982072794/.

V. SHOULD NEW PROPERTY RIGHTS IN DATA BE CREATED?

Politicians in Germany have recently started a debate about the possibility of allocating property rights in data through new legislation.[183] Similar demands have been made in the U.S. and elsewhere in the past.[184] This brings us to the question of whether new property rights should be created for data. One methodology to answer would be to weigh "the reasons why information should be controlled by an owner (locked up)" against "the reasons why information should be not under an owner's control (open for use by others)."[185]

Specifically, this Article analyzes data propertization's effects on the protection of creativity and technological advances and of personal privacy, which are often posited as rationales for "locking" information, and the enablement of freedom of expression and of competition, which are often advanced as bases for keeping "open" the information.[186]

A. CREATIVITY AND TECHNOLOGICAL ADVANCES

As explained in Part III.A, the most widely adopted justification for granting property rights is utilitarian and economic, particularly to incentivize creations and improvements of things that advance technology

---

183 *See, e.g.*, German Chancellor Merkel, Video-Podcast der Bundeskanzlerin #10/2017 (March. 18, 2017) : https://www.bundeskanzlerin.de/Content/DE/Podcast/2017/2017-03-18-Video-Podcast/links/download-PDF.pdf;jsessionid=E48EE1966F5251A9B5832229E0D5ED0B.s6t1?__blob=publicationFile&v=4 (last visited May 10, 2017) (Ger.); Bundesministerium für Verkehr und digitale Infrastruktur, "Eigentumsordnung" für Mobilitätsdaten, www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html, 4.4. (August 2017).

184 *See, e.g.*, Pamela Samuelson, Symposium: Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property?, 52 STAN. L. REV. 1125 (2000); James B. Rule, Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions, 54 UNIV. OF TORONTO L.J. 183 (2004); Tom C.W. Lin, Executive Trade Secrets, 87 NOTRE DAME L. REV. 911, 964 (2012) ("The conceptualization of executive private facts as economically valuable trade secrets further expands on the macroeconomic trend of privacy commoditization.").

185 This balancing model is discussed in the context of propertizing information, particularly as intellectual property, in Margaret Jane Radin, *Symposium: Cyberpersons, Propertization, and Contract in the Information Culture: A Comment on Information Propertization and Its Legal Milieu*, 54 CLEV. ST. L. REV. 23, 25 (2006).

186 Margaret J. Radin, Symposium: Cyberpersons, Propertization, and Contract in the Information Culture: A Comment on Information Propertization and Its Legal Milieu, 54 CLEV. ST. L. REV. 23, 25-26 (2006).

or science. In a study published in August 2017, the German Federal Ministry of Transportation and Digital Infrastructure calls for the creation of "data ownership" as a means to create "data markets" and "data value harvesting."[187] Without property rights in data, companies are less willing to license or share data with other market participants, more likely to hold on to data that they possess and control and less likely to collect data in the first place.[188]

But as shown in Part I, data has grown—and will continue to grow—at an exponential rate, and companies are racing to *create* ever more data, without any "incentivizing" through data propertization. "Open" data, completely without any property rights, has brought revolutionary advances for companies, scientific researchers, medical practitioners, intelligence operations, and many others,[189] ranging countless industries and uses.[190] In recent years, companies have developed various business models that do not rely on property rights (*e.g.*, in the "sharing economy")[191] or rely on intellectual property laws to secure openness and turn their effects on their head (*e.g.*, open source code licensing subject to

---

187 Bundesministerium für Verkehr und digitale Infrastruktur, "Eigentumsordnung" für Mobilitätsdaten, www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html, Part 4. (August 2017).

188 Bundesministerium für Verkehr und digitale Infrastruktur, "Eigentumsordnung" für Mobilitätsdaten, www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html, Part 4 and 5.1.3. (August 2017).

189 *See* Randal E. Bryant, Randy H. Katz, & Edward D. Lazowska, Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science, and Society (Dec. 22, 2008), http://www.cra.org/ccc/docs/init/Big_Data.pdf (discussing how big data computing can and will transform various sectors).

190 *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 393 (2014) ("We are on the cusp of a 'Big Data' Revolution. Increasingly large datasets are being mined for important predictions and often surprising insights. . . The scale of the Big Data Revolution is such that all kinds of human activities and decisions are beginning to be influenced by big data predictions, including dating, shopping, medicine, education, voting, law enforcement, terrorism prevention, and cybersecurity. This transformation is comparable to the Industrial Revolution in the ways our pre-big data society will be left radically changed."); Pamela Metzger & Andrew G. Ferguson, *Defending Data*, 88 S. CAL. L. REV. 1057, 1061 (2015) ("[A] data-driven systems approach has revolutionized other high-risk practices, from trauma surgery to space travel."); Chloé Margulis, *The Application of Big Data Analytics to Patent Litigation*, 99 J. PAT. & TRADEMARK OFF. SOC'Y 305 (2017) (discussing the benefits of big data analytics to the patent industry).

191. *See*, Yochai Benkler, *"Sharing Nicely": On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 Yale Law Journal 273 (2004).

"copyleft").[192] Companies hardly seem to need any further incentives to continue hoarding data.

Whether the creation of property rights in data would encourage companies to share and trade data is far from certain. If global businesses had to deal with individual property rights (which would be national and territorial) on top of privacy and data protection regulations, this would further complicate legal compliance and cooperation arrangements. Data propertization would mean that individual data subjects and owners will have rights to exclude others from using or accessing that data, which will generally complicate and restrict the free flow of information. Individual data subjects may in many cases be identifiable more or less easily, but "data owners" could hold vague and intransparent claims to information that would burden the administration of any "data market" apparently considered by the German government. Based on experiences with patent and copyright trolls,[193] businesses can expect data trolls to get in line to include data they own into studies and data bases to later extract ransoms and nuisance fees based on potential property rights in data.

An example of where vesting property rights has slowed down the pace of research occurred in India when, in response to Western pharmaceutical companies' patenting of products developed from natural resources, the Indian government enacted the Biological Diversity Act, requiring non-citizens and foreign corporate bodies not registered in India to obtain approvals from the National Biodiversity Authority before obtaining any biological resources in India.[194] This had an unintended effect of retarding the potential of India to reap the full rewards of biotechnology, as well as impeding conservation science.[195]

---

192 *See*, Lothar Determann, Dangerous Liaisons – Software Combinations as Derivative Works? Distribution, Installation and Execution of Linked Programs under Copyright Law, Commercial Licenses and the GPL, 21 BERKELEY TECH. L. J. 1421 (2006).

193 *See*, for example, Mark A. Lemley & A. Douglas Melamed, Missing the Forest for the Trolls, 113 Columbia Law Review 2117 (2013).

194 *See* The Biological Diversity Act, No. 18 of 2003, INDIA CODE (2002), vol. 18.

195 . *See* Rohan Pethiyagoda, *Biodiversity Law Has Had Some Unintended Effects*, 429 NATURE INT'L J. OF SCI. 129, 129 (2004), *available at* https://www.nature.com/articles/429129a.pdf; *see also* VANDANA SHIVA, PROTECT OR PLUNDER? 28 (2001).

Data propertization may have negative effects on incentivizing creativity or technological advancements, which is why current property laws generally carve out data from protectable subject matter definitions, as shown in Part III. The U.S. Supreme Court explained in *Graham v. John Deere Co.* that the constitutional authority for Congress to grant patent rights[196] is "limited to the promotion of advances in the 'useful arts,'"[197] which was interpreted as requiring "[i]nnovation, advancement, and things which add to the sum of useful knowledge."[198] The Court held that *existent knowledge* is none of those things and does not promote the advances in the useful arts, and that free access to materials that are *already available* should not be restricted.[199] Similarly, in *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, the U.S. Supreme Court explained that no originality, which is a constitutional requirement for a copyright, can exist for any *fact*—whether it's scientific, historical, biographical, or news of the day[200]— and that copyright law is meant to encourage "others to build freely upon the ideas and information conveyed by a work."[201] These seminal decisions suggest that granting new property rights akin to patent rights or copyrights (*e.g.*, rights to exclude others for a specified period of time) to data, which is *factual* and at best *existent knowledge*, would not promote innovation, advancement of useful knowledge, or public access to information.

B. PROTECTING PERSONAL PRIVACY

The second posited rationale—protection of personal privacy—will also not be advanced by data propertization. Data privacy laws already afford individuals with a nuanced exclusion right, which lawmakers have structured to reflect policy interests in freedom of information and personal privacy with notice and consent requirements, a right to be forgotten, rights against international data transfers, and various other partial or complete exclusion rights. Data subjects could not benefit from

196 U.S. Const. art. 1, § 8, cl. 8 ("To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.")

197 *Graham v. John Deere Co.*, 383 U.S. 1, 5 (1966).

198 *Graham v. John Deere Co.*, 383 U.S. 1, 6 (1966).

199 *Graham v. John Deere Co.*, 383 U.S. 1, 5-6 (1966).

200 Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 347, 348 (1991).

201 Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 347, 349-350 (1991).

an additional data collection or usage exclusion right under property laws, because such a right would be duplicative at best. Companies that acquire ownership to personal data from data subjects like other property could exclude the previous owner - the data subject - from using data about him- or herself. Such an exclusion right would be diametrically opposed to the policy objectives of data privacy laws, which seek to protect human dignity and personal privacy.

Besides exclusionary rights, property laws typically also confer a right to possession, usage, and free disposition.[202] Granting such rights with respect to personal data would also be highly counterproductive to the policy objectives of privacy laws. If data subjects could sell and transfer personal data like other property, the buyers could use and resell their data as they see fit. Individuals already benefit today from their ability to oppose data collection and usage under data privacy laws: companies have to offer attractive services, applications, or other items to gain access to user data in a highly competitive market for users on the Internet of Things. European policy makers bemoan that individuals are not compensated fairly enough for their data by "free" services and apps and want to strengthen individual data sovereignty by mandating that companies pay cash to individuals for their data.[203] But, the administration (and surely taxation) of individual data compensation systems will inevitably create a need for even more data collection, processing, and bureaucracy. If law makers start mandating minimum wages for data subjects, companies will have to charge for formerly-free services and the individuals are unlikely to benefit from the theoretical option to refrain from selling their data. In many circumstances, a property owner will only be able to receive liability-rule protection—which means that the owner can be forced to give up her property (and privacy) in return for an externally-set compensation (often by a court, legislature, or

202 *See supra*, Part III.A.

203 Bundesministerium für Verkehr und digitale Infrastruktur, "Eigentumsordnung" für Mobilitätsdaten, www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html, Part 4. (August 2017).

administrative agency)[204]—and her properties may also be subject to government confiscation or interference without any compensation.[205]

Further, if data can be sold, licensed, and traded like commodities, this would inevitably have negative effects on the protection of personal privacy. In fact, the ability to own and trade personal data can clash with other policies and jurisprudence on ownership relating to humans. Psychologist Raymond Cattell, defines personality as "that which permits a prediction of what a person will do in a given situation."[206] Personal data allows companies, individuals and algorithms to *predict* many aspects of a person's actions, such as where that person wants to go or what that person wants to eat. Proponents of property rights to data at the core of an individual's personality to encourage trade invokes policy arguments against the propertization of humans as discussed in the jurisprudence surrounding ownership of human bodily tissue[207] as well as in human rights and international humanitarian law discourse.[208]

Protection of personal privacy is and can be sufficiently, if not better, achieved with data privacy laws, which are designed specifically to address personal privacy issues.[209] For example, in the EU, as discussed in Part III.I, the legislature put into effect the new GDPR to strengthen individual information self determination by requiring companies to minimize the collection, use, and retention of personal data and by broadly defining "personal data" to cover most categories of data generated by connected devices. Personal privacy is and can be better protected with

---

204 Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J. LAW & TEC 69, 70 (2011).

205 Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J. LAW & TEC 69, 70-71 (2011).

206 RAYMOND CATTELL, PERSONALITY: A SYSTEMATIC THEORETICAL AND FACTUAL STUDY (1950).

207 *See Moore v. Regents of Univ. of Cal.*, 51 Cal. 3d 120 (1990) (holding that a person does cannot retain ownership interest in his spleen as it was a naturally occurring organism).

208 Kofi Annan, *Abolition of Slavery in All Its Forms Remains Major United Nations Priority, Says Secretary General*, UNITED NATIONS PRESS, (Nov. 22, 2002), http://www.un.org/press/en/2002/SGSM8519.doc.htm ("Human beings are not property.").

209 Many scholars debate whether data privacy laws need to be reformed, but that is not a topic considered in this Article. But data privacy laws, whether in their current or amended form, are designed for protecting personal privacy and are more suitable for protecting personal privacy.

data privacy laws demanding data minimization, deletion, and protection, - as opposed to property laws, incentivizing investment and maximization of profits from data collection, sharing, and trading.

C. FREEDOM OF INFORMATION AND SPEECH

Granting property rights to data undermines the freedom of expression. As explained by the U.S. Supreme Court in *Sorrell v. IMS Health Inc.*, information qualifies as *speech* within the meaning of the First Amendment.[210] The Court stated, "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[211] Data propertization—which would allow individuals or companies to control access to their data—would restrict data collection and thus hamper the free flow of information.[212] Thus, "putting a fact into the ownership of only one person, or allowing an entity who generates a fact [] to control how it is used" creates "pernicious dangers" against the freedom of expression.[213]

D. GOVERNMENT USE OF DATA

Restricting information flows could also significantly hinder public governance and law enforcement. As a particularly illustrative and recent example, police officers in a number of US states are required to wear body cameras while on duty, where the recordings are available for inspection as public records.[214] This is part of an important public policy move to enhance transparency within law enforcement bodies and reduce

---

210 *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011); *see also* Jane Baubauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 57 (2014) ("Privacy laws rely on the unexamined assumption that the collection of data is not speech. That assumption is incorrect.")

211 *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011).

212 *See Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011) (holding that a state court regulation violated the First Amendment "because it restricts the speech rights of data miners without directly advancing legitimate state interests"); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 75 (2015) ("[O]ther scholars recognize that restrictions on data collection are restrictions on the free flow of information, which implicate the First Amendment.").

213 Wendy Gordon, Symposium on Bioinformatics and Intellectual Property Law April 27, 2001 – Boston, Massachusetts Data Protection Statutes and Bioinformatic Databases, 8 B.U. J. SCI. & TECH. L. 171, 182 (2002).

214 *See, e.g.*, Nevada's Senate Bill 176 which was signed into law on May 25th 2017.

risks of abusive police practices or unjustified complaints against the police. If police officers and citizens had property rights to the body cam footage, their usage would be greatly complicated. Individual could exclude the *public* from such data, impeding the basic precepts of transparency and accountability that underline this public policy. Many other government uses of data would similarly be impeded by the creation of property rights in data for individuals and potentially companies that buy data from individuals, including census, statistics, taxes, licenses, etc.

E. COMPETITION

Likewise, "propertizing information is designed to restrict competition, if not always by creating economic 'monopolies,' at least by enhancing the position of one competitor vis-à-vis others."[215] For example, ownership in data means that potential users of that data must either purchase access rights from the owner or attempt to gather the desired information themselves;[216] under the second scenario, if the data is a "sole-source data," the owner will not be limited by a price ceiling, which can foreclose all other persons from the possibility of gathering the data independently.[217] This can result in monopolies in data and hurt competition. In fact, there are already attempts to monopolize data, which would only get worse with data propertization. For example, sports leagues increasingly seek to control the dissemination of real-time data in conjunction with lucrative distribution agreements;[218] given that real-time information on sporting events are disseminated through several media,[219] sports leagues' ownership in the real-time information will further undermine the competition from those other mediums.

---

215 Margaret Jane Radin, Symposium: Cyberpersons, Propertization, and Contract in the Information Culture: A Comment on Information Propertization and Its Legal Milieu, 54 CLEV. ST. L. REV. 23, 28 (2006).

216 Wendy Gordon, Symposium on Bioinformatics and Intellectual Property Law April 27, 2001 – Boston, Massachusetts Data Protection Statutes and Bioinformatic Databases, 8 B.U. J. SCI. & TECH. L. 171, 182 (2002).

217 Wendy Gordon, Symposium on Bioinformatics and Intellectual Property Law April 27, 2001 – Boston, Massachusetts Data Protection Statutes and Bioinformatic Databases, 8 B.U. J. SCI. & TECH. L. 171, 182 (2002).

218 Ryan M. Rodenbert, John T. Holden & Asa D. Brown, *Real-Time Sports Data and the First Amendment*, 11 WASH. J.L. TECH. & ARTS 63, 63 (2015).

219 Ryan M. Rodenbert, John T. Holden & Asa D. Brown, *Real-Time Sports Data and the First Amendment*, 11 WASH. J.L. TECH. & ARTS 63, 66 (2015).

F. SOCIAL JUSTICE AND FAIRNESS

Some proponents for data propertization argue that individuals should be able to economically benefit from their data (*e.g.*, monetary compensation).[220] But, consent requirements under privacy and publicity laws already create opportunities for individuals to monetize their statutory choice (by withholding consent except in consideration for valuable services or other benefits), without incentivizing an outright market where individuals transfer ownership to their data to companies, which could then exclude anyone,-including the data subjects and their friends and families,-from using data to which the companies have acquired property rights.

Even if some individuals were able to demand better consideration for their data, most people may lose out. Businesses would have to find alternative sources of funding to pay data subjects and this could ultimately result in disadvantages for consumers. Companies developed many innovative services based on advertising and data-based business models, such as Internet search engines, mobile maps, social networks, video sharing, and consumer reviews, which would never have been able to gain critical mass based on for-pay models. If companies have to switch to for-pay models, because they become unable to run service-for-data models, large parts of the population may lose access to services because they cannot afford them anymore or find the time to focus on personal data monetization to generate additional income.

The present discussion in Germany regarding data propertization also provides valuable insight. As developing countries have made attempts to protect natural resources from exploitation by European explorers in the past, European countries seem now intent on protecting personal data as the "fuel of the digital economy" for European enterprises today.[221] In this

---

220 *See* Kenneth C. Laudon, *Markets and Privacy*, 39 Comm. ACM 92, 92 ("[I]n which individuals can receive fair compensation for the use of information about themselves. This step is necessary because of the continued erosion of privacy brought about by technological change, institutional forces, and the increasingly outdated legal foundation of privacy protection.") The notion that individuals should have the right to own and control data about themselves may have become more popular in reaction to the Snowden disclosures relating to mass data collections around the world.

221 In the EU, politicians debate whether a special right in data should be created as part of the EU's Digital Single Market project. *See* Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee

context, data ownership rights are not claimed for data subjects, but for companies *ab initio*.[222] German scholars have noted that the present movements for data propertization are thinly-disguised attempts to protect the German car manufacturing industry from being disrupted by U.S. technology companies and likened the situation to the previously unsuccessful efforts made by German newspapers and public broadcasting institutions against search engine aggregators.[223] In 2013, the German Parliament had passed an ancillary copyright law aimed at search engine aggregators, in which news and magazine publishers were given exclusive property rights to make press products available to the public unless they qualified as short text excerpts.[224] In response, leading search providers

---

and the Committee of the Regions - Towards a modern, more European Copyright Framework (May 6, 2015), *available at* http://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-626-EN-F1-1.PDF.

[222] For example, German Chancellor Angela Merkel raised the question whether vehicle manufacturers or software developers own data generated by connected cars, but not considering that car owners, drivers or passengers could instead be entitled to own such data. *See* Video-Podcast der Bundeskanzlerin #10/2017, at 1 (Mar. 18, 2017), https://www.bundeskanzlerin.de/Content/DE/Podcast/2017/2017-03-18-Video-Podcast/links/download-PDF.pdf. In contrast, the German Federal Ministry of Transport and Digital Infrastructure (BMVI) released a strategy paper in March 2017, according to which an individual person should have sovereignty over her own data. *See Wir brauchen ein Datengesetz in Deutschland!*, STRATEGIEPAPIER DIGITALE SOUVERAENITAET DES BMVI, http://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html (last visited Feb. 3, 2018) (Ger.) (stating that data is not a "thing" and thus cannot be "owned" in the legal sense under current German property law, but that BMVI wants to develop a solution that leads to an equal treatment of data and things by creating a legal environment in which data can be strictly allocated to an individual or a company as the "owner" of such data.). German Interior Minister, Thomas de Maizière, on the other hand stated that he is against a concept of data ownership in general. *See* Guest Commentary Thomas de Maizière, DER TAGESSPIEGEL (Feb. 16, 2017), http://www.tagesspiegel.de/politik/data-debates-datenschutz-ist-kein-selbstzweck/19391956.html.

[223] Gerrit Hornung & Thilo Goeble, *"Data Ownership" im Vernetzten Automobil*, C.R. 265, 268 (2015) (Ger.). Aala S. Reddy, *The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car*, COGNIZANT (Aug. 2012), https://www.cognizant.com/InsightsWhitepapers/The-New-Auto-Insurance-Ecosystem-Telematics-Mobility-and-the-Connected-Car.pdf; *see also* David Welch, *Your Car Has Been Studying You; Everyone Wants the Data*, BLOOMBERG TECH. (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/your-car-s-been-studying-you-closely-and-everyone-wants-the-data.

[224] *See* Greg Sterling, *German "Ancillary Copyright" Law to Go Into Effect, Imposes Limits on Search Results*, SEARCH ENGINE LAND (May 16, 2013), https://searchengineland.com/german-ancillary-copyright-to-go-into-effect-imposes-limits-on-search-results-159843.

rendered the legislation all but meaningless by carrying only the news of publishers who agreed to waive those exclusive property rights,[225] ultimately causing more disruptions in the German market. The possibility of any legislation on data ownership being similarly circumvented and making a negative impact is another consideration that should be taken into account when determining whether there should be property rights in data.

G. NORMATIVE IMPLEMENTATION OBSTACLES

Besides the lack of compelling reasons for property rights, and the significant policy concerns against creating property rights, any new data property rights regime would face insurmountable implementation obstacles. For example, if sensors on a car owned by a company (*e.g.*, taxi company) generate various "valuable" data relating to the driver (*e.g.*, taxi driver), the passengers (*e.g.*, customers sharing the taxi), and various people that come into the proximity of the car (*e.g.*, people crossing the street in front of the taxi), then who would have ownership rights in that data? Governments, businesses, and individuals would need to claim broad exceptions to broad data property rights in the interest of free speech, information freedom, safety, and security, and courts would inevitably get entangled in litigation that would require constant weighing of property versus speech rights and constant censorship of speech and information flow. Data subjects who successfully sell their data would have to keep accounts for income received and pay taxes. Collective rights societies may come into existence and create new bureaucracies and paperwork. Every data trader would constantly have to issue privacy notices to data subjects or obtain renewed consent, provide individual access, grant portability honor objections and comply with requests to be forgotten under the EU GDPR. To avoid these and other practical

---

225 *See* Matthew Karnitchnig & Chris Spillane, *Plan to Make Google Pay for News Hits Rocks*, POLITICO (Feb. 15, 2017), https://www.politico.eu/article/plan-to-make-google-pay-for-news-hits-rocks-copyright-reform-european-commission/; *see also* Aala S. Reddy, *The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car*, COGNIZANT (Aug. 2012), https://www.cognizant.com/InsightsWhitepapers/The-New-Auto-Insurance-Ecosystem-Telematics-Mobility-and-the-Connected-Car.pdf; *see also* David Welch, *Your Car Has Been Studying You; Everyone Wants the Data*, BLOOMBERG TECH. (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/your-car-s-been-studying-you-closely-and-everyone-wants-the-data; Gerrit Hornung & Thilo Goeble, *"Data Ownership" im Vernetzten Automobil*, C.R. 265, 268 (2015) (Ger.).

problems, data should be left to the public domain, a concept rooted in Roman law as *res nullius*, which means "property of no one," or *res communis*, a public good.[226]

VI. CONCLUSION

No one owns[227] or should own[228] data as such.[229]

Data as such, *i.e.*, the content of information, exists conceptually separate from works of authorship and data bases (which can be subject to intellectual property rights), physical embodiments of information (data on a computer chip, which can be subject to personal property rights; warning symbol painted on a road, which can be subject to real property rights) and physical objects or intangible items to which information relates (*e.g.*, a dangerous malfunctioning vehicle to which the warnings on road markings or a computer chip relate).[230] Lawmakers have granted property rights to different persons regarding works of authorship, data bases, chattels, land and other items for the purpose of incentivizing investments and improvements, a purpose that does not exist with respect to data as such.[231]

Individual persons, businesses, governments, and the public at large have different interests in data and access restrictions.[232] These interests are protected by an intricate net of existing laws that deliberately refrain from granting property rights in data. Existing property laws intentionally *exclude* data from subject matter definitions.[233] Existing data-related laws and property laws balance interests in data and access restrictions based on public policy considerations that would be impaired by a creation of property rights in data.

---

226 See Christopher R. Rossi, "A Unique International Problem: The Svalbard Treaty, Equal Enjoyment, and Terra Nullius: Lessons of Territorial Temptation from History, 15 WASH. U. GLOBAL STUD. L. REV. 93, 117 n.150 (2016).

227 . See Part III.

228 See Part VI.

229 See Part II for distinction regarding information content, expression, physical manifestation of data and information objects.

230 See Part II.

231 See Parts III and VI.

232 See Part IV.

233 See Part V.

New property rights in data are not suited to promote better privacy or more innovation or technological advances, but would more likely suffocate free speech, information freedom, science, and technological progress. The rationales for propertizing data are not compelling and are outweighed by rationales for keeping the data “open.” No new property rights need to be created for data.

Policy Analysis
No. 716 January 7, 2013

A Rational Response to the Privacy "Crisis"

by Larry Downes

Executive Summary

What passes today as a "debate" over privacy lacks agreed-upon terms of reference, rational arguments, or concrete goals. Though the stars are aligning for a market in privacy products and services, those who believe that rapidly evolving information technologies are eroding privacy regularly pitch their arguments in the direction of lawmakers, pushing for unspecified new rules that would cast a pall over innovation. These calls for ill-considered new laws threaten the remarkable economic conditions that have fueled the Internet revolution up until now.

Americans are torn between two historical and cultural traditions about privacy. The Puritan vision of true information transparency on the one hand lives uncomfortably with the frontier's promise of anonymity and personal reinvention on the other. When the Puritan vision encroaches too quickly on the frontier vision, it produces an emotional response—the "creepy factor"—that tends to recoil from innovative new uses of information. But "creepiness" often abates as familiarity grows.

We cannot solve the privacy "crisis" by treating information as the personal property of those to whom it refers or by adapting the systems for protecting copyright, patent, and other so-called "intellectual property" to personal information. But a related body of law explains and rationalizes what is going on with personal information and privacy: the more flexible solution of information licensing.

The licensing model recognizes that most information with economic value is the collaborative creation of multiple sources, including individuals and service providers. Rather than establish enforceable title to property, it assumes joint ownership and licenses specific uses based on mutual exchange of value.

Licensing is already implicit in most information exchanges on the Internet today. With minor enhancement, it could resolve many of today's perceived crises without resorting to inflexible and overreaching legislation.

Larry Downes is an Internet industry analyst. He is the author of the Business Week *and* New York Times *business bestseller,* Unleashing the Killer App: Digital Strategies for Market Dominance *and, most recently, of* The Laws of Disruption: Harnessing the New Forces that Govern Business and Life in the Digital Age.

CATO INSTITUTE

Between Congress, the European Union, and U.S. state legislatures, there are at least a dozen major proposed new laws in the hopper.

Privacy in 2012: State of Disunion

In 2011, I moderated a panel titled "Privacy, Personal Data and Publicness: Where Are We Heading?" at the Privacy Identity Innovation conference (PII).[1] As far as I could tell, we were heading exactly where we are every time we ask that question, which is over a cliff. Between Congress, the European Union, and U.S. state legislatures, there are at least a dozen major proposed new laws in the hopper, many of them aimed at resolving very specific presumed crises that threaten consumer privacy, including "supercookies," geo-location data, targeted advertising, and disclosure of data breaches.

If enacted and enforced, each of these proposals would have severe unintended consequences on the continued evolution of digital products and services. And none of them actually define what behaviors they are trying to regulate, or exactly why. What's the harm being remedied? And why do we think consumers won't continue to make clear what they do and do not want from service providers in the absence of new laws?

Much of this activity was spawned by an alarming report, "Protecting Consumer Privacy in an Era of Rapid Change," issued at the end of 2010 by the Federal Trade Commission (FTC). "[W]hile recent announcements of privacy innovations by a range of companies are encouraging," the Commission staff wrote, "many companies—both online and offline—do not adequately address consumer privacy interests."[2]

The report itself followed a series of free-form roundtables the FTC hosted the previous year, where self-appointed consumer advocates competed to outdo each other in raising the anxiety level over a privacy crisis that they said was imminent.[3]

But the report does little to define which "privacy interests" consumers are concerned about, and therefore what constitutes "adequate" protection of them. Many of the examples that regulators and others most often cite have to do with criminal activity—hacking, malware, identify theft, stalking—those are already illegal and outside the jurisdiction of the FTC. Other concerns have to do with the government's own collection, processing, and securing of citizen information—also outside the FTC's domain.

The 2010 report was preliminary. The FTC followed up in March 2012 with its final report, which reiterated the scary examples, emphasized the vague "principles" it called on companies to embrace, and ended with an overbroad appeal for legislation:

> The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.[4]

Outside the FTC, there's a growing sense in Washington and Brussels that lawmakers need to do something—anything—to allay the privacy panics that pop up with innovative new social networking tools and mobile phone features. "[N]ow we have relationships with large corporations that are obtaining and storing increasingly large amounts of our information," Sen. Al Franken (D-MN) said in one his many recent hearings on privacy. "And we've seen the growth of this whole other sphere of private entities whose entire purpose is to collect and aggregate information about each of us."[5]

"We" don't know specifically what information we're concerned about, in what sense it is "ours," or why collecting and aggregating that information is wrong. But we need, nonetheless, "to legislate and make sure that our privacy protections are keeping up with our technology."[6] The attitude is to shoot first and ask questions later, even as the target continues to move faster than the gun sight.

The blustering of Franken and others highlights what makes most privacy discussions useless from the outset: the term "privacy" itself. The word conjures a great deal of

emotional baggage, as politically charged in its own way as net neutrality, gay marriage, or even abortion. Is it personal information? Intimate information? Identifying information? Or is the question subjective—information that an individual considers private at any given time, defined more by who wants to use the information than anything else? Rarely are two people talking about the same thing when they talk about privacy—not that that slows down the conversation.

One sign of hope that the privacy debate can move in a more focused and rational direction is the changing audience at privacy conferences. Increasingly, there are far more representatives of start-up companies focused on privacy-related services and many more participants from large technology companies, in particular from Europe and Asia.

When the debate was trapped in the bubble occupied by academics, journalists, regulators, and activists, it was just so much performance art. With actual money at stake, however, there are at least experiments that can illuminate what the real problems are, if not the solutions. PII 2011, for example, featured a dozen companies chosen for an "innovator's spotlight," which presented their plans to the audience in several showcases. Ten more start-ups presented at PII 2012.

That shift parallels recent reports that venture capitalists are investing heavily in privacy-related start-ups. In 2010, for example, Reputation Defender raised $15 million; TrustE another $12 million; and SafetyWeb, which lets parents monitor their children's online activities, raised $8 million. Those numbers pale in comparison to the amount being invested in the closely related category of security, but it's still a start.

Despite the difficulty of defining privacy or the nature of the crisis, the technological stars are aligning for a market in privacy products and services to emerge at last. As Moore's Law has worked its magic over the years, the data types and quantities of information that are cost-effective to process have grown exponentially. Static data has been supplemented with transaction data, and devices capable of processing it are proliferating at a fast pace. At this point it's cheaper to save data than it is to delete it, and most users do just that.[7] (The growth of sensors and other low-level devices that can collect real-time information may change that equation in the near future.) Much of the information that is aging—quickly—in aptly named data warehouses never gets queried for any purpose, nefarious or otherwise.

Today service providers are collecting data about each and every transaction in which they participate. It's worth repeating that the consolidation, personalization, and repackaging of that information is not something new or sinister—indeed, it has obvious benefits. It's a significant convenience not to have to reenter static information every time one returns to a website to browse, shop, pay bills, or search.

The more data collected, the more it can be used to improve everyone's transactions. Everything from eBay's seller ratings and other crowd sourced evaluation systems to Amazon's and Apple's recommendations based on similar purchases of similar buyers wouldn't be possible without the collection and processing of consolidated transaction data.

But with the personal computing revolution, the Internet, social networking, and the cloud, transaction data is now being dwarfed by the collection and processing of transient, and often intimate, information; a kind of Joycean stream-of-consciousness of the whole world. Much of it is entered into the datastream by users themselves. As of mid 2011, Twitter was processing 200 million tweets per day. It measures increases in the 1000s of percents.[8] Facebook averaged 3.2 billion "Likes" and comments generated by its 900 million users every day during the first quarter of 2012.[9] And who can count the number of blogs (let alone blog comments), emails, and other information-detritus?

Without much encouragement, and certainly no obligation, we are using social networks to digitize vast quantities of personal (though largely irrelevant and economically useless) information. Most of it can hardly be thought of as private, nor is there any risk that its inadver-

Today service providers are collecting data about each and every transaction in which they participate.

tent disclosure or use could harm or offend anyone but the truly paranoid. You post a link on my Facebook page to an article from a website that you read and found interesting. I check in at the office on FourSquare. A follower retweets your submission to the "things I learned from horror movies" trending topic. Who cares?

Well, some people care, although they have a hard time explaining why. There's a vocal minority who feel that any information collection, retention, or processing is an affront to personal autonomy and should be heavily regulated if not banned.[10] Activists want Web users to be allowed to sign up for "do not track" lists.[11] They want companies to disclose to all users every possible use of every possible data element before they collect it, and only collect it after a consumer has "opted in." In the foreseeable future, we may see proposals that every app on your mobile device stop before each data collection or processing activity to reassure itself of your continued consent.

What these rhetorically attractive ideas ("notice"; "transparency"; "choice") conveniently leave out of the equation is their immediate and catastrophic effect on the key innovation that made the commercial Internet so popular and so successful in the first place: advertising-supported services. Most websites are free to users. Google offers a nearly complete portfolio of application software and charges its users for almost none of it. So do Facebook, Twitter, LinkedIn, Groupon, and the rest of the old and new generations of Internet businesses. Search our databases! Store your email, photos, and videos on our servers! Make video calls with our software!

What motivates these businesses to drive as much traffic to their servers as possible? In the network economics of information, the more you exploit them, the more valuable their companies become. But not because users pay them directly. Rather, it is because their use makes the services more valuable to others.

For the most part, of course, those others are advertisers. The revolution in free services and software that has unleashed much of the computing genius of the last decade has been built largely on the back of advertising.[12] In 2011, for example, Google earned 96 percent of its revenue, or roughly $28 billion, from advertising.[13] And there was nothing new about that success—the earlier media revolutions of radio and television were financed exactly the same way.[14]

With most Internet services, the user is the customer, but the revenue comes from those who have an interest in accessing the right users. And the more accurate and detailed the information that service providers collect, from the largest possible user base, the more valuable the information becomes. So the incentives are there for service providers to make their products more compelling all the time, both to attract larger groups of users and to provide opportunities for those users to engage ever more deeply with the products, generating ever more data with which to impress advertisers.

Analyzing how many users a service has, how much time they spend with it, and what interesting things they do while they are there are skills at the core of successful Internet companies. Understanding user behavior, after all, translates to more ad spends and higher ad rates, generating both competitive advantage and revenue.

The importance of robust and detailed user information cannot be overemphasized. Unlike e-commerce sites selling products, social networking applications don't exist at all without user information—Facebook, Twitter, Yelp, even Craigslist and eBay are literally nothing without user-supplied content. Attracting users, giving them more things to do, and keeping them happy are not just customer service imperatives. They're a matter of life or death.

It's important to dispel right from the start some persistent myths about how advertising actually works. The marketing of transaction data is far more complex than advocates for more government regulation of privacy would have us believe. It's not "your" information that's being sold. First, the information is collected and stored by the service with your permission. If the data ever was "yours," you freely traded your interests in it. For most of the Internet's billion users, the exchange is a good one, generating

There's a vocal minority who feel that any information collection, retention, or processing is an affront to personal autonomy and should be heavily regulated if not banned.

far more value for users than the costs of supplying and parting with the information.

Data being processed for advertising isn't "yours" in a second sense: It doesn't identify you as the source. Search engines such as Google don't sell information about what individuals searched for, and advertisers don't then turn around and advertise to those individuals based on what they have learned about them. Google doesn't even know "who" is doing the searching, only that the searches originated from the same computer. Google keeps track of the activities of that computer (which could be used by one person, a family, the patrons of a library, or a bot), and it does so only by storing cookies on the computer that maintains the connection.

But the cookie doesn't contain identifiable information about the user—the name, address, and so on. And once you delete a cookie, the data collection has to start all over again. (Your searches will get less streamlined if you do, as Google's software will make worse guesses about what you're actually looking for.)[15]

More to the point, ads you see on Google search results or other applications only appear to be optimized as personal messages. In most cases, the services and their sponsors don't make use of the individual cookie data, or at least not on its own. Say you searched for "carpet cleaners in Berkeley, CA." Google doesn't sell that fact to carpet cleaners in Oakland, who then pass along an advertisement to the computer of whoever typed that search. The actual science of advertising is both more and less sophisticated than that.

For advertising to work, suppliers need the preferences, habits, and transactions of large numbers of users, which are consolidated, mined, and analyzed to find patterns and common behavior. (Gender and zip code are the most valuable pieces of identifying information—names and addresses are of little help.) Once all that information is compiled, it can be compared to the practices of a particular (but unidentified) user, who can then be served with ads more likely to be relevant to his interests. The better the science, the more the advertising appears to be personal. But it's still only the illusion of personal.

Focus is valuable to consumers as well as advertisers. More focused ads mean sellers waste far less time advertising the wrong things to the wrong people.[16] Nineteenth century retailing pioneer John Wannamaker famously said that half his ads were wasted, he just didn't know which half.[17]

Not much has changed. I keep a recycle bin right next to the mailbox, where nearly all of my delivered mail goes without being opened. I'm not against ads; I'm against ads for things I don't want. And I often don't know what I want until I see an ad that helps me realize which is which. Steve Jobs famously said, "A lot of times, people don't know what they want until you show it to them."[18]

Put another way, advertisements are offers. Those that are perceived as "ads" are offers that are at least slightly off. But an ad for the right product or service, offered at the right time to the right person at the right price, isn't an ad at all. It's a deal.

Personal results—or rather, results that appear personal—require group input. That's where the real value of data collection is, not in separating out the information of any particular individual. On their own the Amazon purchases of one customer are of little use in helping the company suggest other products that are likely to be of interest. That data must be compared to the purchases of everyone else before the "targeted" response can be meaningful.

The more data collected, the more valuable the collection, and the less reliance placed on the individual's data. In that sense the more information we allow to be processed, the more privacy we actually get in the form of obscurity. That, of course, is just one of the many privacy paradoxes that confound regulators and worry businesses.

Historical Roots of Privacy Panics: Hester Prynne vs. Davy Crockett

Understanding how information is actually collected and used would go far toward

Search engines such as Google don't sell information about what individuals searched for.

For most consumers and policymakers, privacy is not a rational topic.

freeing the "privacy debate" from the rhetorical sinkhole in which it has been trapped. Yet having that conversation seems impossible. Why? The short answer is that for most consumers and policymakers, privacy is not a rational topic. It's a visceral subject, one on which logical arguments are largely wasted. Americans seem wired to react strongly and emotionally just at the mention of the word "privacy," or the suggestion that some new technology is challenging it.

What sets in seems more often than not a panic response, as we worry that the game is up and our last remaining shred of personal autonomy has just been undone by products and services we don't understand, in part because they didn't exist yesterday and are only in prototype today. As science fiction author Arthur C. Clarke wrote in 1961, "Any sufficiently advanced technology is indistinguishable from magic."[19] And we know how locals often respond to those who wield magic.

Consider one example of the life cycle of a privacy panic: the blow-up in 2011 over Apple's geolocation files on the iPhone. Researchers "discovered" a file on the iPhone that appeared to be keeping track of cell towers and WiFi hotspots (not, as many said, GPS data) used by the device. Journalists and lawmakers jumped to the conclusion that the file was tracking the locations where the user's phone had actually been, making it possible for Apple to "spy" on its customers. The "secret" nature of the file, plus the potential for embarrassment if its contents were revealed by Apple (perhaps to law enforcement, perhaps to a divorcing spouse, or perhaps just out of spite), raised an alarm.[20]

The story exploded into immense proportions within hours, with news outlets reporting user outrage[21] and members of Congress, fuming, calling for hearings[22]—and, at the hearings, for new legislation, enforcement actions by the FTC,[23] and other corrections to what was clearly a privacy apocalypse.[24] Apple said nothing for a few days—researching, it turns out, what the file actually was—leading to even more anger at their corporate arrogance.[25]

In the end the whole thing turned out to be nothing. The file wasn't storing information about where the user had been, or even where the phone had been (Apple doesn't know who is holding the phone, obviously). The file was part of a crowdsourced database of connection points that other phones with similar usage patterns had made use of recently. It was being stored on the iPhone in the event that the user invoked a service that required knowledge of the phone's location (directions, area restaurants, etc.).[26]

The file was just a backup in the event a ping to the GPS satellites didn't work or responded too slowly. As the company made clear, "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so."[27]

But logic and facts play little part in an emotional response. A week after Apple explained the file's true nature, I spoke on an NPR news program with Sen. Al Franken and the FTC's chief technologist, Ed Felten.[28] Both of them continued to describe the incident as one where Apple was tracking the location of its users and failing to disclose that fact. Whether they simply hadn't read Apple's explanation or didn't believe it, both acted as if the answer had never been given.

Franken, who had already scheduled a hearing, stuck to his script: "We had this thing with Apple with iPhones and iPads," he said on the program, "that were tracking your location and then storing it in an unencrypted way on a file, and let's say you hooked up to your own laptop and all that information then went on your laptop, so it had stored this information for, you know, almost a year of pretty much everywhere you'd been with your device. And we're talking about other kinds of mobile devices as well and privacy concerns."[29]

But Apple was not tracking "your" location, or even of the location of your device. It wasn't tracking anything at all. Both of them should have known better, and almost certainly did. But the story was too good, and the visceral reaction too powerful not to use in pursuit of unrelated interests. In Franken's case, it's the passage of some new privacy leg-

islation—he seems not to care especially which of several proposals moves forward. For the FTC, the greater the panic over privacy, the more likely the agency will get new authority and new funding to enforce new rules. Like any enterprise, they want to increase their market share.[30]

The vagueness of demands for new laws and regulations would be comical if it weren't so dangerous. Americans don't know what they want when it comes to privacy; or rather, that what they want depends on when and how the question is asked. We want to protect victims of domestic abuse from being stalked, for example, and so we insist that search engines, cell phone providers, and social networks delete identifying information immediately. But we also want the police to catch those who are doing the stalking, and so we also insist that information collectors retain identifying information.[31]

The result is a regulatory whipsaw. In 2008 the House Energy and Commerce Committee pressed Verizon, AT&T, Time Warner, Comcast, Microsoft, Yahoo, and Google to reduce the length of time they retained customer transaction data, which many of the companies voluntarily agreed to do.[32] Yet in 2011 the House Judiciary Committee advanced a bill (with 40 cosponsors) that would require these same companies to increase the length of time they retained the exact same data, and make it available without a warrant to law enforcement agencies investigating a variety of crimes.[33]

Even without actual lawmaking, simple threats have led to unhelpful responses. Under pressure from the House in 2008, for example, Yahoo changed its data retention policy from 13 months to 3 months.[34] But when Congress and the Department of Justice pressed for longer retention in 2011 in the name of effective law enforcement, the company changed its policy again, this time from 3 months to 18 months.[35] Context is everything, and the context is only clear after the fact. But laws and regulations by their nature deal with future situations. We're therefore doomed to be, generally speaking, unhappy. Or at least uneasy with any legal remedies.

There may be some solace in recognizing that there's nothing new about these privacy paradoxes. American culture has long maintained inconsistent attitudes toward privacy, simultaneously embracing secrecy and transparency with equal passion.

The source of that dichotomy has deeply historical roots. On the one hand, the whole point of frontier life (which many historians believe defines the American experience) was the ability to go west, shed personal baggage from your past, and redefine yourself however you wanted. The kind of "rugged individualism" practiced by Henry David Thoreau and extolled in the essays of his friend Ralph Waldo Emerson meant one was judged by his deeds, not the accidents of his birth or his past. Davy Crockett, whose modest achievements as a frontiersman, congressman, and soldier were elevated to mythic status as the self-made "King of the Wild Frontier," perhaps best epitomizes the spirit of the wide open American West.

Ranchers and farmers could be as anonymous as the height and opaqueness of their fences,[36] and as eccentric, too. If the neighbors got too nosey, one just moved farther west. Joseph Smith, founder of the Mormon religion, believed himself to be a prophet, a view that was met with hostility in his native New York. Smith moved west to Ohio, Missouri, and then Illinois, where he was assassinated.[37] So his followers headed for the wilderness and settled in Utah where they could do as they felt compelled without interference, at least until the line of settled frontier caught up with them decades later.

Back East, the original colonies were largely settled by Puritans, who practiced a particularly extreme form of what today is referred to as transparency. God saw everything, so why not the rest of the community? Perhaps the most evocative picture of the lack of privacy in early American life is the one painted in Nathaniel Hawthorne's *The Scarlet Letter*, where Hester Prynne's punishment for extramarital sex (evidenced by the birth of her child) is to be forced to wear a giant letter A (for adulterer) on her chest.[38]

American culture has long maintained inconsistent attitudes toward privacy.

The digital revolution has all but erased the cost barrier to collecting and processing social information.

That the father of her child is the town's fire-branding preacher, who speaks most passionately against Hester, is Hawthorne's way of suggesting the hypocrisy of the transparent Puritan village. But hypocrites or no, these were some seriously mandatory social networks.

Frontier and Puritan America coexisted in a kind of uneasy peace, with the law of the East occasionally visited on the lawless West, which was mostly left alone if for no other reason than the cost of enforcement. The federal government unsuccessfully attempted to suppress the "Utah Rebellion" in the 1850s, for example, but it was not until completion of the transcontinental railroad though Salt Lake City in 1869 that pressure began to build on the Mormons to abandon polygamy and accept a secular government. The Church banned polygamy in 1890, and Utah became a state six years later.[39]

With the closing of the American frontier (Frederick Jackson Turner pegged the date at 1890[40]), one would have thought the Puritans would reassert Calvinist transparency on the whole country. But the industrial revolution brought forth other ideas. The anonymity of the frontier was replaced by the anonymity of city life.[41] In the metropolis, there were just too many people to keep track of or to assert moral authority over.

Hester Prynne would have been free to walk the streets of 19th and 20th century Manhattan anonymously. No one would know or care how she lived her life, which would perhaps be fatal. Where *The Scarlet Letter* captures the claustrophobia and hypocrisy of Puritan village, the archetypal story of dangerous anonymity and isolation in industrial life is that of Kitty Genovese, a New York City resident who was brutally raped and murdered in an alley in 1964 while neighbors all around did nothing, not even calling the police. The story has been exaggerated and mythologized, but even its persistence as myth underscores modern fears that industrial life dehumanizes urban residents.[42] That is, it gives them too much privacy, to the point of anomie.

Before social networks and smartphones, cities were impersonal, amoral, and paranoid. Early in Joseph Heller's 1974 novel, *Something Happened*, the narrator captures the spirit (or dispirit) of the company man: "In the office in which I work, there are five people of whom I am afraid. Each of these five people is afraid of four people (excluding overlaps), for a total of twenty. . . . "[43] And so on until it becomes clear that everyone in New York is afraid of everyone else.

In economic terms, we could say that early urban life raised the cost of collecting, storing, processing, and accessing the kind of information we need to decide whether or not to network with each other. Absent computers and digital technology, the price was too high. The default—that is, the lowest-cost response—was to do nothing, whether to call the police or to trust one's coworkers, let alone strangers. "Mind your own business" is an equation as much as it is a cliché.

Meanwhile, the Puritan ideal lived on in the suburbs, where, according to an equally persistent mythology, people kept their doors unlocked and everyone knew everyone else's affairs. Whether that was a utopian myth (*Leave it to Beaver*) or a dystopian one (*Peyton Place*) depended on, well, depended on nothing, really. Americans have always been comfortable supporting contradictory views of privacy and its pluses and minuses.

In both town and country, however, the digital revolution has all but erased the cost barrier to collecting and processing social information. Now that we can have it all, we're unavoidably faced with a true privacy paradox. On the Internet, we live in both city and suburb, Puritan village and frontier wilderness, at the same time. We want—demand—our privacy, but we also expect to be able to share whatever information we want, from the sublime to the ridiculous, with whomever we want, and to do so free of charge. Often, the tension between these two powerful desires leads to contradictory behavior and conflicting legal standards.

The Puritan part of our minds (the part that invented capitalism, according to Max Weber[44]) wants to know everything about everyone else, the better to decide whether

and how to interact with them. Transparency is a virtue, and not just for corporations and governments. The more information we can collect and process about everything and everyone, the easier it is to decide with whom to interact and how to behave. Information, on this view, is the lubricant that keeps the machinery of society humming.

The frontier part of our minds, on the other hand, wants the option to be anonymous on demand, "to be let alone" in the famous formulation of Samuel Warren and Louis Brandeis—or the "right to be forgotten" as it's now being called in Europe.[45] The frontier mind recognizes, although often vaguely and viscerally, that there is something profoundly American about keeping to oneself, and it resents the intrusion into our personal lives of anyone we don't explicitly invite (an invitation that can be revoked either on whim or further reflection).

The pioneer view of personal autonomy was a central motivator for many of the groups who migrated to the United States, including, oddly enough, the Puritans, who had suffered enough interference with their beliefs and practices by the Crown to pack up and sail to the New World.

That peculiar version of a right to privacy—asserted against the government but not each other—is baked into the U.S. Constitution. Many of the most potent safeguards provided by the Bill of Rights in particular limit the ability of governments to demand information from the people. In response to the heavy-handed practices of America's colonial overseers in England, for example, the Fourth Amendment prohibits unreasonable search and seizure of "persons, houses, papers, and effects."[46] The First Amendment bans Congress from legislating on matters of religion or speech,[47] two aspects of individual identity that are particularly "private." The post–Civil War amendments expanded the Bill of Rights, extending its protections to former slaves and including state and local governments in bans that had originally applied only to the federal government.

But, again, these privacy protections explicitly bar intrusions by the government. The Constitution says nothing that even suggests a limit on how much information can be collected by businesses or other citizens, no matter how intrusive or how it is used. Except for a few specifically legislated exceptions, Americans have no general right to privacy against anyone other than the sovereign.

So Americans have always experienced privacy as a kind of Manichaean duality. Perhaps that explains why every survey taken on attitudes to privacy in the digital age suggests Americans are deeply concerned about their personal information online even as they casually give up whatever data is asked of them, often with no idea who is doing the asking or the purpose of the collection.[48]

The external conflict between Puritan and frontiersman, between Hester Prynne and Davy Crockett, has now been internalized. We're capable of living with our discomfort, which is saying something. We demand the right to have our every trivial thought broadcast to the Twittersphere, and to have attention paid to it. And then we recoil in panic at novel technological developments (geolocation tracking, super cookies, and facial recognition) that expose some new aspect of ourselves to the world.

The internal conflict often masks innate hypocrisy. Many people want privacy from outsiders but reserve the right to demand full disclosure from those with whom they interact on a daily basis. But what's good for the goose is good for the gander. Those who most adamantly insist on legal tools to erase their past would likely be outraged were they the victims of someone else's false or misleading presentation of self.

You may not want future creditors to know about your poor payment history, or for potential employers to find out about your criminal record, or for someone you hope to date hearing about your previous marriages. But these are essential facts if others are going to, respectively, loan you more money, hire you to a position of responsibility, or move in with you. The desire for privacy is often a desire to protect ourselves from the negative

Many people want privacy from outsiders but reserve the right to demand full disclosure from those with whom they interact.

consequences of our own behavior.

In that sense, privacy isn't a human right—it's a limit on the rights of those who have to deal with us. Privacy comes at a price. The more of it we have, the more risk to which we expose everyone else. In commercial transactions, banks and insurers offer protection against that risk (often at a steep cost). In social interactions, all we have to fall back on are limited safeguards of tort law, which assigns liability to dangerous behavior only if it causes calculable harm, and criminal law, which punishes the most egregious acts, including assault, theft, and large-scale fraud.

There have been periodic efforts in U.S. history to expand the constitutional right to privacy from government intrusion into a broader protection that can be asserted and enforced against technological innovations employed by businesses, the press, and other individuals. For the most part, however, these efforts have failed to overcome the Puritan's economic and cultural biases for transparency. Warren and Brandeis, for example, began their crusade in response to the novel challenge raised by newspaper photos exposing the social and personal lives of the well-to-do. But they never argued that their revolutionary "right to be let alone" actually existed in American jurisprudence. Instead, they hoped that outrage with an overly familiar press would rally general support for new laws to create it.[49]

Following publication of "The Right to Privacy," some state courts did tinker with new legal claims for "false light," "invasion of privacy," and other privacy-related torts. But efforts to create a general right to privacy largely sputtered out. And as the U.S. Supreme Court moved to shore up First Amendment protections for a press under siege during the Civil Rights movement, whatever was left of these novel rights was further marginalized.[50]

Today, the U.S. press and other nongovernmental actors enjoy wide freedom to report true facts, even those obtained through invasive technologies that would have seemed inconceivable to Warren and Brandeis. The Constitution has spoken: the need to know even personal details of the lives of our celebrities, including political and cultural figures large and small, outweighs Warren and Brandeis's desire for new laws to ensure "propriety" and "decency."[51]

Privacy isn't a human right—it's a limit on the rights of those who have to deal with us.

Measuring the Creepy Factor

Today's privacy crisis is a function of innovation that happens too quickly. Given the accelerating pace of new information technology introductions, new uses of information often appear suddenly, perhaps overnight. Still, after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy. The first reaction, what I call the "creepy factor," is the frontier response. It doesn't last long. The Puritans reassert their rational order more quickly all the time.

As noted earlier, large-scale data collection, like the urbanization of America, in some ways contributes to privacy even as it challenges it. The more information available about more people, in other words, the more privacy we get as anonymous members of various groupings. Perhaps the biggest reason for today's resurgent and generalized privacy anxiety is that it just doesn't seem that way. When a novel information service *appears* to have zeroed in on one's deepest darkest secret preferences, it's hard to resist a strong emotional response. But there is almost always an explanation that, when understood in context, takes the creepiness out of the equation.

How, for example, did Google know when I searched for "War Horse" that I was looking to buy tickets to a performance of the play in San Francisco? (Answer: my IP address identifies the service provider for my computer as Comcast in Richmond, California.) How does CNN know who my friends are, and what stories on the CNN website my friends have recently read? (Answer: my friends tagged the stories on Facebook, which actually controls that part of the screen.)

Better targeting of ads and other content,

unfortunately, often evokes a visceral response, one that is by definition not rational. When we imagine the specter of a kind of corporate Big Brother, the frontier mind kicks in, ready to saddle up and head west to avoid the prying eye of Puritanical software. Or worse, it can lead us to fretful and panicked calls for immediate legislative solutions that would reign in what are in fact entirely innocent and impersonal technologies that only simulate invasive human behavior, and that do so to our economic and social benefit.

Gmail users, for example, see ads along the top and side of the screen advertising products and services that often relate to the contents of recent emails and conversations. It's all software. We know intellectually that there's no vast army decamped at some Google Ministry of Love reading through the messages looking for opportunities to connect them to contextual advertising. But the software has gotten so good at interpolating our messages that it begins to look personal.

That's the moment when the creepy factor comes into play. Something happens that you didn't expect, or hadn't experienced before, and you think, "How did they know that?" Right now, my Facebook page is showing me photos of three people "you may know." I know all three. For two, the connection is obvious. For the third, the connection is eerily indirect. Until I understood what mundane data elements connected all three to me, I felt uneasy about Facebook. The company seemed to be an actual person, and a sinister one at that.

As we record more information in digital form in hopes of sharing it with our intimate contacts and less enthusiastically with advertisers who pay for the services we love, it's inevitable that more of these visceral responses will occur. When specific data is used in novel ways, the initial response is often to be creeped out.

So let's try to take the emotion out of the equation, or, at least, account for it in hopes of a more rational conversation about what, if anything, needs to be done to manage the creepy response. We can begin by restating the problem simply: the more personal the information used by an advertiser or service provider, the more emotional our response to its use:

$$P \rightarrow E$$

where P = personal and E = the degree of emotional response.

The creepy factor, however, is the response to a novel use of information to provide a seemingly personalized response. Over time, the creepy factor decreases. Most users are now accustomed to customized Google search results, specific Gmail ads, and prescient Facebook recommendations. They no longer creep us out. The diminishing emotional response can be represented by dividing the degree of emotional response by a second variable, F (familiarity), so:

$$P \rightarrow \frac{E}{F}$$

If consumer response to a particular information practice does not become less emotional over time, this suggests that the negative response is not a function of novelty but of genuine discomfort. Put another way, an information use that does not seem less creepy over time may be one that consumers believe imposes more cost to privacy than it provides in benefits elsewhere. That still doesn't mean a regulatory intervention, specific or otherwise, is required. Regulations impose costs of their own. Often the more efficient solution is for consumers to vote with their feet, or these days with their Twitter protests. As social networking technology is coopted for use in such campaigns, consumers have proven increasingly able to leverage and enforce their preferences.

In Europe, the default rule is almost the reverse—governments don't wait for true market failures, but instead protect vaguely defined general privacy rights against corporations on behalf of the citizens. This is one reason, and an important one, that most data processing innovations of the last 25 years have taken place in the United States. Entrepreneurs who

The creepy factor is the response to a novel use of information.

want to launch a new application or service that collects, analyzes, and processes information need not apply to any government agency for permission.

Indeed, for companies in the United States, adopting any kind of privacy policy (except as their service may apply to children) is entirely voluntary. The FTC can only bring enforcement actions when a company promises to treat information one way but actually uses it in another, and only when such behavior rises to the standard of an "unfair or deceptive" misrepresentation that causes actual harm; that is, when it approaches the legal definition of fraud.[52]

When new applications stimulate our creepy response (and more of them will enter the market all the time thanks to the technology trends mentioned above), the critical policy question then becomes what we do during the initial, emotional response period, when creepiness is high.

Consumers either adjust to new information use or act through the market to change the practice.

In the absence of premature interventions by regulators, in nearly every case consumers either adjust to what is an essentially inert new information use or act through the market to change the practice. Consumer-enforced change is frequent—recent examples include the cancellation of Facebook Beacon and Google Buzz, and Apple's modifications to the geolocation files stored on consumer devices. When consumers objected strongly to how these services were using information, the companies either modified their practices or canceled the service altogether.

In 2011, to take a specific example, LinkedIn users revolted against a new feature called "social ads," in which ads for a particular product or service included the profile photos of contacts in a user's network who recommended it.[53] The creepy factor was apparently too high, and the company quickly agreed simply to list the number of network members who recommended the advertised product.

The recommendations of one's contacts could always be seen by reviewing their individual profiles, but combining that information with ads apparently crossed a line. "What we've learned now," said Ryan Rolansky, the company's director of product development, "is that, even though our members are happy to have their actions, such as recommendations, be viewable by their network as a public action, some of those same members may not be comfortable with the use of their names and photos associated with those actions used in ads served to their network."[54]

This may be an example where constructive engagement with a service provider led to quick resolution—true market success. On the other hand, it's possible that with a little more familiarity to LinkedIn users, the creepy factor would have dissipated, and on balance provided more benefit than cost. The more "social" the ads at LinkedIn, after all, the more the company can charge its advertisers, keeping subscription fees lower and encouraging a larger and richer network.

Choosing the more expensive solution was a trade-off LinkedIn users made, but it was still better than forcing through new laws banning the use of photos in ads or some similar remedy. In response to another privacy panic, California recently passed a law prohibiting employers from forcing employees or job applicants to provide access to their "social media" accounts. But as legal scholar Eric Goldman points out, the law, while well-intended, was poorly drafted, and is certain to cause negative, unintended consequences if not corrected. For one thing, "social media" was defined so broadly that it effectively covers all electronic content, whether personal or employment-related.[55]

For those who naturally leap first to legislative solutions, it would be better just to fume, debate, attend conferences, blog, and then calm down before it's too late. Future innovations hang in the balance.

Unfortunately, the mainstream media often fans the flames of the emotional response, raising the value of E. The press has strong financial incentives, after all, to amplify and echo the creepy factor once it appears. That, at least, has been the repeated experience of the last decade. Outrageous stories of corporate and government information malfeasance are surefire attention-getters. It's no surprise that privacy-

related stories are often cast in that light, even when the facts are nowhere near so clear-cut.

Consider the *Wall Street Journal*'s What They Know series,[56] written by veteran reporter Julia Angwin. Angwin's award-winning stories investigate the actual information collection and use practices of a wide range of corporate and government entities, ranging from the largely innocent to the simply criminal. What they Know is a rare example of investigative journalism in technology reporting, and the source of important findings and discoveries.

While the series has helped to stimulate more mature conversations about privacy, its rhetorical style is often counterproductive. Angwin regularly stacks the deck and oversells the lede, crossing the line from reporting to commentary. Consider a *What They Know* story from 2010, which carries the headline "The Web's New Gold Mine: Your Secrets."[57]

The headline alone signals both a point of view and a conclusion. Is information collected by websites "yours"? And is it really "secret" or did you reveal it, perhaps over time or in different component parts? The phrase "gold mine," likewise, conjures an enterprise that, when successful, will generate enormous profits relative to cost. We know before reading the story that whatever gold is being mined, the miners are not to be trusted.

But headlines are not the story. Let's look at the first sentence:

> Hidden inside Ashley Hayes-Beaty's computer, a tiny file helps gather personal details about her, all to be put up for sale for a tenth of a penny.

The article, in case you didn't guess from the lede, is about the use of cookies. Cookies are data files that Web browsers store so that sites can record information about navigation and use by the particular computer on which the cookie is stored. When a user of that computer returns to the site, his or her browser sends the site a copy of the cookie, which allows the site to customize itself—highlighting links that have previously been clicked, for example, or pre-populating sign-in or other data fields with prior entries.

A strong connotation of this sentence is that factual information about Ashley is traded at a low price, passing hand-to-hand among heaven-knows-who, on a shady personal information market. This is a common, mistaken assumption about how advertising works.[58] In fact, it is advertising networks that use the information to direct ads her way. The only way for the companies doing the advertising to discover personal information about her is for her to click on one of their ads and begin interacting with them.

Whatever the ethical implications of more advanced uses of cookies, they have been a technical feature of web browsers from the beginning. Their useful attributes cannot be seriously doubted. They have never been held to be illegal.[59]

So does my navigation of a site's pages really constitute my "secrets"? Are mouse clicks even "personal" details? (The data in a cookie is not linked to a specific, identifiable person, as the story later makes clear.) Are cookies "hidden" from users "inside" our computers? (They can be viewed and deleted through the browser's control options; they can also be refused generically or by type of requesting site.) In what sense are they "tiny," and why does that matter?

According to the article, cookies and "other surveillance technology" "know" things about "you." They collect "your information" ("yours" both in the sense of being about you and being property which belongs to you), which is then "sold" to advertisers. This seems neither surprising nor dangerous, but in the hands of a skilled advocate, even the most inert technology appears weaponized. A few paragraphs on, Angwin writes: "One of the fastest-growing businesses on the Internet, a *Wall Street Journal* investigation has found, is the business of spying on Internet users."

Well that is certainly one interpretation of the article's findings, and clearly the one Angwin and her editors want readers to draw. From the article's details, however, what actually seems to be new—what the *Journal*'s investigation "found"—is that service providers are

In the hands of a skilled advocate, even the most inert technology appears weaponized.

The Internet is just picking up where television once blazed a trail.

getting better at making economically beneficial use of the data that cookies and "other surveillance technology" have been collecting all the time. Beneficial to users as well as marketers, no less. Again, the ads pay for the free services.

Journalists are certainly free to beat their readers over the head. Most *Journal* readers, I suspect, prefer writers who lay out the facts and let them draw their own conclusions—or at least wait until the facts are established before editorializing in a news story. Given the general climate of creepy factor responses to Internet privacy, Angwin's language doesn't simply push the emotional button—it wires it to a car battery. To the extent that "What they Know" has discovered misleading, fraudulent, or otherwise illegal activities, Angwin rightly deserves the accolades her series has received. But why not give readers credit for being able to decide for themselves when data collection and use is good, bad, or somewhere in the middle?

Just as an exercise, let's rewrite that first sentence in neutral language, and see how the facts uncovered by the investigation lose some of their menacing implications:

> The Web browser on Ashley Hayes-Beaty's computer is set to accept cookies, files that site operators use to keep track of how users navigate their pages, both to save time on return visits and to offer more relevant advertising that helps pay for Web sites' operations.

Because most of the uses of personal information that trigger the creepy response are related to advertising, it's also worth noting that what's going on here isn't so much new as it is an improvement. Rather than simply pushing products, marketing long ago shifted to wrapping products inside solutions to larger consumer problems. Ads are now designed to appeal to more basic human aspirations or anxieties, and to suggest, often subtly, that the advertised product will fulfill or resolve those feelings.

The clearer a particular demographic group's feelings are understood, the better the ad can target their needs. That's all that's really involved in targeted or behavioral advertising—it uses contextual information to place a consumer in a group with common characteristics (age, sex, zip code) and then directs ads to them that are more likely to speak to that group.

The Internet is just picking up where television once blazed a trail. In the 1960s, television became the ubiquitous technology of what Marshall McLuhan called "the global village"—the prototype for social networks.[60] Those who are fans of "Mad Men" get the advertiser's view of the origins of targeted or behavioral advertising, albeit one filtered through a cloudy highball glass.

For marketers, the direct and visual properties of the medium made it possible to get inside the heads of viewers in ways print and radio simply couldn't approximate. Marketers, in short, learned to stop selling products and start selling solutions, often to deep-seated problems.

Consider some of the taglines from the early days of TV: "Does she or doesn't she?" (gray hair/aging). "We bring good things to life" (electric appliances/modernity) "Even your best friends won't tell you" (mouthwash/bad breathe). If those problems are actually existential and unsolvable, so much the better—consumers (the modern understanding of the term originates here) would have to keep buying forever, urged on by the promise of "new and improved."

The creepy factor was born in these ads. Watching television in the 1960s, it may have frightened viewers to see a commercial for instant coffee or laxatives or dandruff shampoo that emphasized the angst of the pre-purchasing characters—those who made bad coffee or had flakes on their clothes, just as they worried they also did. How did the television know what was making (some of us) anxious?

But over time, we adapted and moved on. We look at those old commercials now with nostalgia. How quaint and how impersonal they seem. But at the time they were nothing short of revolutionary, and even scandalous.

I have personal experience with the creepy factor, as most everyone does. In the early 1980s, I was a regular business traveler, taking four to six flights a week as part of my job as a systems engineer for a large consulting firm. I was a charter member of many airline frequent flyer programs which, like the Google+ and Spotify of their day, were initially by invitation only.

It was a foregone conclusion that that information would be put to some use other than keeping track of when free flights had been earned. As the programs quickly matured, the airlines developed systems to track the flight histories of customers. The first uses were internal—to fine-tune routes and schedules, and to offer passengers discounts and other specials to try to shape travel behavior, first for the airlines and soon for their hotel, rental car, and restaurant partners.

Here's where it got creepy. I was traveling a great deal between Chicago and Silicon Valley, almost exclusively on United Airlines, which had the best schedules between Chicago and San Francisco. One day I received a letter from the manager of the Fairmont Hotel in San Francisco, where I had never stayed.

"Dear Mr. Downes," it read. "We know you travel frequently between Chicago and San Francisco, and we'd like to invite you to stay at the Fairmont on your next trip." The letter offered some discount or freebie.

Of course I knew that the letter had been generated by computer, using a simple extraction of United's Mileage Plus database for Chicago customers with frequent trips to San Francisco. The list may never have even been made available to the hotel, but more likely to a third-party mailing service, which actually produced and sent the letter. The manager didn't write the letter or sign it; he certainly never saw it. No human other than me likely did.

Knowing this didn't help. There was something about the letter that went over a line I didn't even know I had drawn. I didn't mind that United knew where I was going. And I didn't mind their giving my address (there was, of course, no email in those days) to their hotel marketing partners. I wasn't heading to San Francisco for any purpose about which I was embarrassed or which I needed to keep secret. But still, there was something disturbing about the manager of the hotel "knowing" my specific travel history and contacting me about it. Something I couldn't explain rationally.

During that period I was a member of the board of directors of the ACLU in Chicago, where I lived. So I understood that although the airline had crossed a line that offended me as a customer (and I let them know, for whatever that was worth), they had broken no law.

The situation, it's worth noting, would have been different if the same kind of data sharing had taken place between two branches of the U.S. government—say, for example, the Federal Aviation Administration and the Internal Revenue Service. Under the Privacy Act, federal agencies may not "disclose any record . . . to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." Had the IRS used flight manifests from the FAA to target business expense audits, my reaction would have been considerably different. I would have sued.[61]

This suggests a further enhancement of the creepy factor equation. The degree of the emotional response we have to a novel use of personal information is often determined not so much by the use itself but by who is using it. The more distant the user is from one's immediate circle of intimates (friends and family), the more likely the new use will generate an uncomfortable emotional response. Or, to put it another way, the more unpredicted the use, the higher the creepy response. This suggests variable U for user:

$$P*U \rightarrow \frac{E}{F}$$

Or in English: the more personal the information, amplified by the degree of disconnect with its user, the more emotional the response to a novel use—but still diminishing over time with increasing familiarity.

The more unpredicted the use, the higher the creepy response.

That added variable highlights one of the most serious defects in what passes today for a public policy debate over privacy and how we should or should not surround it with legislation. Privacy is often a matter of context—information that seems perfectly natural for friends and family to have may have a higher creepy factor if it's being used by companies with whom one does business, even higher if it's being used by companies with whom one does not do business.

It's fine for you to know that today is my birthday, but if the grocery store somehow figures it out and sends me a special coupon, I'm going to flinch pretty hard. How did they know? What else do they know? Why do they care? Creepy.

The creepy factor goes up even more, at least in the United States, if the user is a government agency. And the most unwelcome form of information use is by criminals or for otherwise destructive purposes. If the information is being used to defraud me, or by a stalker or a bully, or to trick me into accepting viruses or malware on my computer to be passed along unknowingly to friends and family, there's no hint of a transaction with mutual benefit. Economists don't like transactions that don't add value to anyone. In law, we call them crimes.

Information use, let alone philosophical concepts such as "privacy," can't be regulated in the abstract. Aside from the problem of identifying what is and is not private (or even personally identifying), the use of the information has to be judged against the purpose of the user. Even within the broad categories of users suggested above—friends and family, familiar businesses, unfamiliar businesses—there are uses that are and are not acceptable that depend on context. If you're signing up for a free newsletter, there's no reason why a website would need to know your telephone or credit card number. (In fact, if they ask, it raises suspicions about the legitimacy of the site.)

Determining acceptable and unacceptable uses of information is often highly subjective.

But obviously if you are trying to buy something, it's understandable for a merchant to ask for that information, along with a shipping address. Likewise, questions about health are extraordinarily intimate, but how else to get diagnostic help from a medical service?

Consider Ancestry.com and other online genealogical services. These are companies who, without anyone asking and without anyone's permission, have collected vast databases of deeply personal histories that, if the service has done its job, cover just about everyone's family tree—bad seeds and all. Yet rather than complain about this multi-generational invasion of privacy, users pay for the privilege of using it. The service is only valuable if the company has done a good job of invading the user's privacy ahead of time—a service for which, in the genealogy context, the consumer is willing to pay.

As these examples suggest, determining acceptable and unacceptable uses is often highly subjective. There may of course be general categories of use that many people would agree to—or at least agree are unacceptable. No one would think it appropriate for Netflix to include questions about communicable diseases or digestive problems as part of account signup.

No matter—even if users don't think explicitly of the costs and benefits of giving up certain information in certain transactions, the creepy factor is always lurking in the back of their minds, a kind of binary switch that, if thrown, will click the magic "X" in the corner of the browser window and make the discomfort go away.

That's the problem with debating privacy legislation. We don't know and can't say *ex ante* which information that refers to us or our transactions is "personal" (in the emotional sense) or "private," nor can we say which uses of that information we'll find pedestrian and which we'll find invasive, and how long it will be before we get used to it. It is, after all, an emotional response, which makes rational discussion difficult if not futile.

For better or worse (almost certainly better), Internet users are hooked on the "free" software, content, and services that rely for revenue on information collection and use. So are the service providers. So we need to figure a way to head off a looming crisis of faith about what data is being collected and how it

is used—a crisis that goes under the unfortunate misnomer of "privacy" when it is really about economics and who gets to extract value from information. There are a few interesting proposals to consider—one not so good and the other much better.

A Bad Solution: Privacy as Property Ownership

Warren and Brandeis proposed to combat technological advances in data collection and distribution with a new enforceable right of privacy. But the plan failed. As legal innovation limped along, slowed in large part by latent or overt First Amendment concerns, technology galloped ahead. A similar fate seems likely for much of the current crop of proposed privacy protections. Even if they pass, they are likely to be so specific to particular uses and technologies ("pop-up ads," "spyware") that by the time they can be enforced they will have become anachronisms.[62]

So it's worth asking if there's a more efficient and effective way to resolve our conflicting views of information use—to quiet the internal struggle between Puritan and frontiersman. How, in other words, can we lubricate social interactions with accurate information without too often triggering the creepy factor's visceral response?

One possible solution is to remove emotion from the debate by characterizing personally identifiable information as a kind of personal property that individuals own, subject to market transactions for use and transfer. By turning information into property and assigning the initial ownership to the individual to whom the information refers, the idea goes, privacy would become just another form of "intellectual property" like patents and copyrights. The propertization of privacy is an old idea, going back at least to a 1993 article by Sheldon Richman.[63]

Support for the ownership of personally identifiable information comes from a wide range of legal scholars, including Lawrence Lessig, who summarized the arguments for and against this approach in an article that advocated for it.[64] Lessig argued that information use today is subject to the whims of those who collect it—too much so. Without property rights assigned in the first instance to those to whom information refers, it's difficult to characterize use of that information without permission or compensation as what he believes it really is: stealing. "If people see a resource as property, it will take a great deal of converting to convince them that companies like Amazon should be free to take it. Likewise, it will be hard for companies like Amazon to escape the label of thief."[65]

There is an obvious appeal to this approach. It takes privacy out of the realm of posturing and amped-up creepy-factor reactions and into an area of law and policy that is established and rational. The creation and management of property rights are as old as the oldest legal traditions in Western Europe. Treating intangible information as a kind of property and applying analogous principles to its ownership, use, and transfer is likewise deep-rooted, going back at least to 1710 and the Statute of Anne, which established copyright in England. There is tradition here, as well as precedent. There is also considerable understanding of both the effectiveness and limitations of such systems.

The property rights solution is elegant and logical: assign property rights to consumers for personally identifiable information, then give them the tools to manage and enforce those rights, including, if they like, to sell them. If a coalition of government agencies and responsible corporate users can get together and establish enforceable property rights over private information, anarchy will subside. Emotion disappears; problem solved.

Those arguing for the ownership of privacy are on the right track but for the choice of metaphor. It is certainly true that information can be thought of as a kind of property—initially assigned to one party, and then bought and sold through market transactions. But there are a few problems. Most consumers—indeed, most economists—only understand property in its tangible form, and have trouble applying

It's worth asking if there's a more efficient and effective way to resolve our conflicting views of information use.

It is certainly true that information can be thought of as a kind of property. But there are a few problems.

the very different economic principles that apply to intangible property, which includes all forms of information. Accounting for intangibles on corporate balance sheets, for example, is still in a primitive state of development, despite the increased importance of intangibles in determining corporate value.[66]

The explicit analogy between information ownership and the current state of copyright and patent law makes the problem messier. Over the last few decades, cynical and counterproductive extensions to the terms of copyright and mechanisms for enforcing it have poisoned consumers against any coherent understanding about what it would mean to "own" privacy rights or the like.[67]

Likewise, the increased generosity of patent offices, particularly in the areas of software and business methods, has bred a counterproductive culture of patent trolling, expensive litigation, and interference with innovation. Patents are no longer seen as a beneficial form of propertized information, even among companies who hold them and economically minded legal scholars.[68]

The general concept of "intellectual property" has been tainted, perhaps irredeemably so. Including "private" information under that heading would complicate more than it would clarify.

Another objection to the ownership approach is its unexplored assumption that the initial allocation of a property right should go to the individual to whom the information refers. That starting point isn't obvious. While the information we are talking about *refers to* or *describes* a particular person, that does not mean that the person actually exerted any effort to create the information, or that they have done anything to make it useful in combination with the information of other individuals. You spend money, accept credit, and pay your bills, but that doesn't mean you've done anything to make a useful record of your credit history future lenders can evaluate.

So we might instead think that those who unearth, normalize, store, and process information ought to be the initial owners of any property rights to it. For one thing, they need the economic incentive. Why else would a company go to the trouble of collecting various public and private records of your payment, employment, and asset history in order to create a credit profile? Under the view of Lessig and others, the moment that profile was of any value, its ownership would be assigned to the individual to whom it refers.

If that were the property rights system for privacy, no for-profit entity would bother to create credit profiles, which require not only an individual's information but the ability to compare it to the information of large groups of similar and dissimilar consumers. And unless you live your life paying cash for everything, you need someone to compile that history. Otherwise, there's no basis for a lender to determine the appropriate risk for a loan. Your lender will either make no loans or charge exorbitant interest rates. This is a central defect in Lessig's assumption and the less sophisticated claim by some privacy advocates that you "own" information simply because it refers to you.

Initial allocation can be crucial, and Lessig has picked the wrong starting point. We know this from the work of Nobel prize-winning economist Ronald Coase and the so-called "Coase Theorem." As Coase explained in a seminal 1960 essay, the initial assignment of a new property right will not matter if the market for trading the right is functioning without friction.[69] Since markets never function without friction, Coase concluded that the initial allocation of any property right should be the one that results in the least amount of avoidable overhead, or what Coase had earlier termed "transaction costs."[70]

In his famous example, he considered a new railroad that ran along the field of a farmer. The train engine gives off sparks as it passes, causing fires that damage the farmer's crop. Does the farmer have the right to be free of the sparks, or does the railroad, which operates under the transportation laws of the state, have the right to be free of liability?

For Coase, the question was not one of fairness or morality, but rather of which rule led to the most efficient use of resources for

society as a whole. Coase reached the startling conclusion that in a perfect market system, it wasn't necessary to decide who should have the initial allocation. If the farmer had the right to be free of sparks, the railroad would be willing to pay for the privilege of polluting an amount somewhat less than the value the railroad received for running additional trains, or running them at higher speeds and therefore causing more sparks. If that amount was greater than the damage to the crops, the right would change hands.

On the other hand, if the railroad began with a right to pollute, then the farmer would be willing to pay an amount somewhat less than the cost of the damage to his crops to have the railroad attach spark-arresting devices to the engines. If that amount was greater than the cost of the spark arresters, again, the right would change hands

These examples assume that there are only a few parties involved, and that there are no costs associated with negotiating, drafting agreements, and enforcing them—the transaction costs. That's where Lessig's approach gets into trouble. In Lessig's view, every individual should begin with a property right to all information that refers to them. If corporate users want it, they will have to negotiate a price for it. If the price is too low, consumers won't sell, and the information will remain private. If the right deal is reached, the information will be transferred, and will no longer be private.

But electronic information being collected today on the Internet and elsewhere involves billions of users and perhaps thousands of different data collectors. Up until now, the default practice, at least in the United States, is that transactional information (identifiable or not) can be collected unless the user opts out—either by selecting particular privacy options or by walking away from the interaction when a service starts asking for the wrong data. And that's fine, because most consumers are comfortable with the data being collected most of the time. (We know that because the Internet, unlike the rest of the economy, is still growing quickly, fueled by consumer information.) It also makes economic sense—it's the allocation that leads to the fewest transaction costs and therefore the least amount of overall social loss.

Flip the allocation around and the system comes to a crashing halt. If data can only be collected on the basis of a negotiated agreement with each individual consumer (and perhaps each individual data element), the transaction costs go through the roof. Indeed, for the most part those costs would be far greater than the value to either party of completing a trade. Transaction costs higher than the value of the transaction put an end to hopes for a market for any kind of property, private or otherwise.

That's the problem with simple-minded proposals (I don't include Lessig's proposal in that category) to "just" change the default rule on the Internet from opting out of information collection and instead to requiring each user to opt in with each data collector, or perhaps even with each specific use. If consumers want to be tracked, the proponents argue, then why not require them to say so explicitly?

The reason is that the effort to educate oneself on the pluses (free services) and minuses (a much smaller Internet) of participating, and determining the fair market value for information collected largely for future uses, would overwhelm most consumers. Far fewer interactions would take place, and those that did would take more time and effort by consumers. The transaction is roughly the same, but the transaction costs would be fatal.

No doubt there are some Internet users—true frontiersmen, perhaps, with little love of Puritan transparency—who would be willing to give up on ad-supported free services in exchange for complete anonymity. Such users would either have to pay directly for the services—search, email hosting, photo and video sharing, social networks, music and television programming—or go without them. They may even prefer that model to today's wide open Web.

But changing the default rule to allocate the initial right to decide the structure of the Internet would come at the cost of inconveniencing everyone else. We might make such a policy decision if we understood all the pros

Most consumers are comfortable with the data being collected most of the time.

If everyone had the right to forbid the use of any private fact, basic institutions, notably the press, simply couldn't operate.

and cons, but it's disingenuous to argue, as many privacy advocates do, that there's no real difference between the two approaches.[71]

Let me give a concrete example of the problem of transaction costs. Of the experiments in new privacy rights the common law courts engaged in after Warren and Brandeis's article, one is the "right of publicity." The right of publicity allows famous people to prohibit uses that they do not license of their likenesses, voices, or names in advertising. This is the only right that survives today with much force, especially in states such as California and New York with large, politically influential populations of celebrities.[72]

This rule isn't so much a right for the famous person to preserve their anonymity as it is to change the initial allocation of information-use rights. Rather than treating the name and recognizable likeness of a celebrity as public information, in other words, it requires an advertiser to negotiate for its use with the celebrity (or possibly the celebrity's heirs). And it applies only to use by an advertiser or other who wants to trade off the fame created by the celebrity's efforts. News sources can still name the celebrity, and anyone can still utter true facts about the celebrity.

The risk of a broader rule of privacy, one that applies to any historical or descriptive fact about any individual, is a problem of monopoly. If I allocate to the individual a property right to any fact that relates to or describes them, then I have only one possible party to bargain with for the use of that information. The risk is high that the individual will misjudge the value of their individual privacy and simply refuse any price. What would be otherwise economically valuable transactions won't occur, leading to what economists call "dead weight loss."

That monopoly problem doomed many of the new rights, including the torts of "false light" and "invasion of privacy," that some state courts tentatively embraced in the early 20th century. Judges quickly realized that if everyone had the right to forbid the use of any private fact, basic institutions, notably the press, simply couldn't operate.

Consider the example of Luther Haynes.[73] Haynes, far from a celebrity, was a sharecropper who moved to Chicago from Mississippi in the 1940s. There he married a woman named Ruby Daniels, but the marriage later fell apart due in part to Haynes's drinking, overspending, and neglectful parenting. The couple split up, and Daniels descended into poverty and the horrors of early 1960s public housing and other Great Society programs.

We know all this and quite a bit more about Haynes from *The Promised Land*, an acclaimed nonfiction book by Nicholas Lemann.[74] Though the book is principally an account of the migration of African Americans to the North, Lemann tells it through the example of Ruby Daniels, a dramatic story of the human costs that, Lemann suggests, were paid by millions like her.

The problem was that Daniels' privacy—which she willingly gave up to Lemann as part of his research—was in some sense the joint property of Haynes, who did not participate in the book. By the time *The Promised Land* was published in 1991, Haynes had cleaned up his act. He had stopped drinking, had remarried, and was a deacon in his church. He and his new wife were deeply embarrassed by the truthful but painful disclosures in the book, and he sued Lemann and his publisher in federal court, arguing that Illinois law (where Haynes lived) still recognized invasion of privacy.

Had the disclosures in *The Promised Land* involved public figures such as government officials, the First Amendment would have given Lemann wide berth to report them and would have protected him from liability even if he had gotten his facts wrong. So long as his investigation did not sink below the "actual malice" standard of *New York Times v. Sullivan*[75]—which held there can be no action for defamation unless the paper knew of the untruth or recklessly failed to investigate it—Lemann would have been immune from paying any damages.

Haynes was no public figure, but in any case the facts he complained about were true. So Haynes's principal legal claim was for in-

vasion of privacy. (Ironically, as with all legal cases claiming defamation or related privacy torts, bringing the lawsuit ensured more publicity of the private facts, and this time in freely quotable public records.)

Reviewing the history of that tort in Illinois, appellate judge Richard Posner concluded that the state had never fully embraced it. If it survived at all as an actionable offense, he wrote, invasion of privacy was limited to the disclosure of much more intimate facts than Lemann's book had described—perhaps the specifics of the couple's sexual practices. Haynes was out of luck.[76]

I was working as Judge Posner's law clerk when the appeal came before the court, and I confess that I felt deep sympathy for Haynes. After all, he didn't ask to be a figure in Lemann's book; he had achieved notoriety simply because Lemann's research had led him to Haynes's ex-wife. Haynes wanted the court to recognize what the Europeans might call his right to be forgotten, to have his early life erased so that his friends, family, and employers would judge him solely on his present conduct. Imagining embarrassing facts from my own youth, my response to Haynes' predicament was high on the creepy factor.

But difficult cases, as the saying goes, can make bad law. The problem with the right to privacy that Haynes wanted to enforce, as Posner correctly concluded, was that its cost to society was far more than the cost to Haynes's reconstructed reputation. Haynes was asking for monetary damages for his injury, but might have equally asked the court to forbid publication of the book until the publisher removed all references to him. As a monopoly holder of a property right to facts about his past, Haynes likely wouldn't have traded his right for any amount of money. That would have been the danger in allocating the right to him, and the reason Illinois courts, Posner concluded, would not do so.

Haynes, of course, was just one person, and Lemann's publisher could surely have afforded to pay the damages he requested. But had Haynes prevailed in his lawsuit, it would have signaled to authors of nonfiction books that they could not write about any individuals without their permission—permission many if not all individuals like Haynes would never grant.

Lemann needn't have written specifically about Haynes; he was just unlucky enough to have once been married to Ruby Daniels, a subject the author found compelling enough to anchor his narrative. But presumably everyone in similar circumstances described in the book would have also refused to sell a property right to privacy, had they had one. With the allocation of rights assigned to the person to whom information refers, nonfiction writers would be limited to writing in the abstract, or creating composite characters, exposing them to claims that their work wasn't concrete and therefore wasn't convincing.

It's also worth noting that the facts Haynes wanted to suppress were facts that also described the life of his ex-wife. Daniels, the victim both of Haynes and the welfare system, wanted her past exposed, not for purposes of retribution against Haynes but to have her deeply powerful struggle validated to Lemann's readers. When facts relate to information, even intimate information, about more than one person, how would a property right be allocated? Would it be shared property, owned equally by everyone referenced? If not, would any one person hold a veto, as Haynes argued he did, denying all the others the ability to sell, trade, or otherwise dispose of true facts as they wish?

Monopoly, joint ownership, and other transaction cost issues suggest that the more socially efficient initial allocation of a property right to private information should begin with the entity that collected the information in the first instance. But how then would the property right ever shift to the individual to whom the information refers? How, for example, could you "buy back" your credit information and take it out of circulation, assuming you wanted to do that?

In part, the answer is legislation that already reduces the transaction costs of managing some financial information between users and individuals. Under the Fair Credit

When facts relate to information about more than one person, how would a property right be allocated?

Reporting Act (FCRA), for example, consumer reporting agencies cannot collect certain information, including accurate but dated information. They must also correct errors—that is, inaccurate information, even if it is not personally identifiable information.[77] This is an example of the kind of information regulation that can work: (1) targeted to a specific kind of information, use, and user; (2) identifying clear consumer harms from inaccurate or negligent information collection; and (3) remedies that are both enforceable and directly responsive to the harms.[78]

Under the FCRA model, a market is created in which individuals can repurchase their financial reputations. To buy your way out of unpleasant but true negative financial facts—late payments, frequent changes in employment, and other risks relevant to future creditors—you need to invest in improving your reputation. That requires not a payment to the credit bureau but the discipline of practicing the kinds of financial responsibility that generate positive facts. Over time, these outweigh and replace the negative ones.

Let's take some other examples. What if I decide that the profile Amazon has compiled about me and my preferences has taken an uncomfortable turn, and the company is now suggesting or advertising to me products that I am interested in, but either wish I wasn't or am embarrassed to see revealed, even to me? Similarly, what happens when my choice of TV viewing trains my DVR to record suggested programming that I would rather not have suggested to me (in my case, too many cooking shows and superhero cartoons—accurate, but awkward)?

Here the process of buying back my privacy is cheap and simple. For Amazon, I can simply cancel my account and open a new one with a different user ID. (Amazon does not require me to provide authentication that I am a particular person, only that I am authorized to use whatever credit card I use to make purchases). It's even easier with my DVR. I just reinitialize the device and erase all the locally stored data that has been collected. (Likewise with cookies and other tracking tools for the Web.) I lose the usefulness of the services that work with that data, but I can easily retake control of the relationship and, in doing so, my privacy.

Transaction costs aside, the joint ownership of the facts Luther Haynes hoped to suppress raises a more fundamental problem with the property rights proposals of Lessig and others. When they speak of individuals being the initial owners of "their" information, just what information are we talking about? Lessig and others answer "personal information" or "private information." But these answers simply beg the question.[79]

Problems of definition in the property approach run deep.

Problems of definition in the property approach run deep. Is "my" information any information that I enter into some application; that is, information that I first translate to digital form? Or is it information that refers to me in an identifiable way, regardless of whether I had anything to do with its creation? Or only information that somehow defines an existential sense of self—information that refers to me in a deeply personal, intimate way? Are the addresses of websites I visit private information? The inventory of items I buy from you? The photos I take of members of my family?

Information "on" me, a Senate staffer said at a recent privacy conference, "is mine. It's not yours." Good rhetoric, but not much of a basis for defining property rights. Much of the information collected "on" me isn't private or even personally identifiable. It only has value when someone else goes to the trouble of codifying it, often without any effort from me.

FTC commissioner Julie Brill, perhaps recognizing the lack of interest most marketers have in individual data, includes in her definition of protectable information "not just the raw data, but also how the information has been analyzed to place the consumer into certain categories for marketing or other purposes." Her view of transparency is not just providing the consumer with access to "their" data, but also with the algorithms for processing it.[80]

There are problems with all three alternatives. The category of information I initiate or create is both under- and overinclusive. I in-

troduce all sorts of data into the cloud. While some of it is both personal and sensitive, much of it is utterly mundane—a review on Yelp, a bid on eBay, a click on a link on my Yahoo! homepage (recorded through a cookie) or a Google search result.

At the same time, much of the most personal information about me is entirely created by others, often using a great deal of private information that refers to other people. A credit score is a calculation that is based on data collected by credit card companies, banks, employers, and others and is only useful when it can be compared to the credit scores of others. (Is 680 a good score? I can't answer that without knowing the percentage of consumers that have higher and lower scores.) Would I own the credit score (and perhaps those of everyone else whose data was needed to create mine), even though someone else went to all the cost and trouble of preparing it? Would I own the list of all the links I clicked on? Neither? Both?

Falling back to the third alternative—information that is existentially private, that is, information that defines who I am—undoes the goal of propertizing privacy and taking it out of the realm of the abstract and illogical. For now I have left the world of neutral, unemotional property rights, bought and sold on the open market. Information that is private because it intimately and deeply defines who I am as a person is the least valuable and least likely to be legally exploited (blackmail is a crime). It is also the most subjective and the most contextual. I can't define it, to paraphrase Supreme Court Justice Potter Stewart in a famous case about obscenity, but I know it when I see it. We're right back to the creepy factor.

For most people, the contents of some if not most email to friends and family would almost certainly be categorized as private information. But what about more abstract data, such as the number of email messages I send in a particular period of time, or the route a certain message takes getting from sender to receiver, stripped of actual content or subject or even the identifier of the sender and receiver? Though these data may be associated with me in an identifiable way, most people would agree that there's nothing private about them. What is personal, it turns out, is in the eye of the beholder, or rather, in the eye of those who perceive me and use the information to identify and evaluate me.

We don't know what kinds of information Lessig and others have in mind when they propose that legislation should create a new property right and allocate its initial ownership to "you." That will make it difficult to satisfy the goal of privacy ownership in the first place—to create a market for buying and selling that right. Systems of property require certainty as to the kinds of rights associated with ownership.

In traditional property systems, such as real estate, certainty is reflected in the idea of holding "title," or proof of ownership. As anyone who has ever bought or sold a home, car, or other valuable piece of property knows, the cost simply to determine title (and in real estate, to insure against an incomplete title search) can be significant—again, likely more than the value of the transaction itself in the case of many less-significant information exchanges.

This brings up a more serious drawback to the property rights solution. In real estate, as in personal property, there is also certainty as to the thing to which the right attaches (the "res" in legal terminology). I either do or do not have title to my house and land, but what constitutes the house and what constitutes the land can be easily determined. For the house, a visual inspection is all it takes. For the land, a visit to the county records office, where the metes and bounds of the parcel is defined and the chain of title recorded.

Information is different in a significant way. We can't see data; we can't hold it in our hands. To say that I own my data doesn't mean the same thing as saying I own my car. If it is data about me that was created by a company or government entity, I may never even know that it exists. The data is likely stored in multiple copies and formats in the cloud. Each copy is identical and equal in value to every other copy. There is no scrap or salvage value to information.

To say that I own my data doesn't mean the same thing as saying I own my car.

The more a piece of data is used the more valuable it becomes.

Information, as noted earlier, belongs to a very different category of goods and services that economists refer to as intangibles. Trademarks are intangibles. So are patents. The goodwill of an ongoing business, from an accounting standpoint, is an intangible, and so is peace of mind. (We're certainly willing to pay for it.) All information, private and otherwise, is intangible.

Under the law, intangibles can and often are treated as a kind of property, and in many cases they have been for decades. The problem with applying property rights to information is that intangibles have different and often counterintuitive economic characteristics from tangible property. Unlike physical goods, for example, intangible property can't be easily controlled by the owner. It is "non-excludable," to use the economic term.

Information, Stewart Brand famously said, wants to be free. Brand meant free in the sense of not costing anything, given the trajectory of Moore's Law.[81] But information also wants to be free in the sense of being unhindered in its migration to use that is economically valuable. In either case (or both), once information takes a digital form, it is very hard to control who uses it, or to enforce a system of payment for its use, even one with criminal sanctions. Just ask any copyright holder.

Digital information also differs from tangible goods in that it can be duplicated into an infinite number of identical copies at little to no cost, allowing consumption by additional users. In most cases the duplication doesn't reduce its value. Economists refer to that feature of information as "non-rivalrous."

The more a piece of data is used the more valuable it becomes, like a television program or a novel, or the nonproprietary, open standards that define the Internet itself. We can all use it, manipulate it, and remix it, all at the same time. The more it is used, the more popular it becomes, and that popularity can often be monetized. This property is what economists call "network effects."

When we're done, the information, unlike a barrel of oil, is still there, perhaps more valuable for having been used. The Internet's protocols weren't worth much when only a few government and academic computers made use of them. Now that billions of devices rely on them every nanosecond, their value is incalculable. And yet no one pays anyone else for their use, at least not directly.

That's not irony. It's just a very smart decision to eliminate the transaction costs of charging for use of the standards in order to maximize network effects. As a result, users build something much more valuable on top of them. Indeed, it's the main reason the Internet protocols (IP) became today's dominant network standard, rather than more sophisticated but proprietary alternatives offered until very recently by leading computing and communications companies. Every company whose profits rely on the existence of the Internet is, at least in part, monetizing the value of the standard.

Information is non-excludable and non-rivalrous—the opposite of tangible property. It is difficult for economists, let alone consumers, to keep in mind the different economic principles that apply. That makes creating a new market for property rights to private information, if nothing else, a difficult problem in norm generation. We'd have to teach consumers that there are two kinds of property, and which of their possessions fall into which category.

If the upside-down economic properties of intangibles wasn't hard enough for users to understand, there is the added problem, noted earlier, that the idea of information as property has been tainted by misuse of a set of laws that grant special property rights to creative information—by which I mean trademarks, patents, trade secrets and, worst of all, copyrights. This group of laws is often referred to as "intellectual property," a term that has been used intentionally to confuse users into believing that protected information is not intangible but is literally somehow a kind of physical property, whose unauthorized copying constitutes "theft" or "piracy."

Before the digital age, the intangible features of intellectual property, especially copyrighted works, didn't much affect their

economic or legal treatment. That's because creative works couldn't be experienced without first translating them to a physical medium—a book, an 8-track tape, or a canister of film. We experienced the information only through possession of a physical copy and specialized devices that "played" it.

Information embedded into media couldn't be "free" in either sense of the word, which made it easier to control but more expensive to distribute. The costs of the media were so significant, in fact, that they have long been the dominant characteristic of creative enterprises. Journalists don't work for information services, they work for newspapers. Songs were available not in music stores but in record stores. The whole industry defined itself with reference to the physical copies—it wasn't creative information; it was "mass media." "The medium," as Marshall McLuhan cryptically said, "is the message."[82] The costs of creating and distributing content so dominated the supply chain, in other words, that the creative part often didn't seem especially important to those in the industry.

When copies had to be made in physical form, the economics of tangible goods dominated. You owned a physical copy of a movie, but you didn't own any rights to the movie itself—you couldn't adapt it for another medium, you couldn't produce a sequel, and most of all you couldn't make and sell additional physical copies.

The migration of information products from physical copies to digital distribution has, at least in theory, made it easier to think of copyrighted works in particular as intangible property. But producers, distributors, and retailers of physical media confused consumers by promoting the idea that owning a (decaying, fragile, and soon-to-be-obsolete) copy was equivalent to owning the underlying, intangible content. (How else to convince consumers to replace one generation of media with the next one?)

At the same time, advertising-supported content made it possible to deliver music on the radio and programming on television to be free of charge over the public airwaves. "Free" content underscored the idea that the only information that was valuable was information that could be held in some media product. The result: a generation or more of consumers who simply can't understand that information really is intangible.

Media and software companies, who themselves may not be so clear on the concept of intangibles, have made things worse with their long-standing campaigns to criminalize unauthorized reproductions. That was another side-effect of Moore's Law. When content required physical media, unauthorized copying was expensive and easy to uncover. You needed industrial equipment to make the copies, a distribution network to get them to market, and access to retail channels to sell them. Each of these steps, to be successful, exposed the unauthorized copier to discovery and the application of both civil and criminal sanctions.

The digital revolution, however, removed nearly all of the costs of copying and simultaneously created virtual manufacturing, distribution, and retail outlets that were superior[83] and, at least with early examples such as Napster and Grokster, largely untraceable. To put it mildly, the content industries freaked out. The Recording Industry Association of America went so far as to sue their own customers. None of them could have paid the statutory fines, and few understood that what they were doing was any different from listening to the radio.[84] The strategy neither slowed the unauthorized reproduction of musical compositions nor collected significant damages for technical violations of U.S. copyright law.[85]

All that the RIAA's lawsuits (and those more recently by the film industry) have done is create a new language that paints any effort to tap the astonishing potential of digital distribution as both a sin and a crime. Services that help users find torrented content are "rogue" websites "trafficking" in "pirated" copies. Users who listen to songs without paying for them, or who try to listen to songs they have paid for in a different medium, are "thieves" "stealing" content. Unlocking devices or programs to remove limitations on their use are said to be "jailbreaking."

When content required physical media, unauthorized copying was expensive and easy to uncover. The digital revolution removed nearly all of the costs of copying.

Licensing has proven to be a much more flexible legal and economic system for dealing with intangibles.

Whatever one thinks of these efforts to police information use, this is the language of tangible, not intangible, property. When it comes to information, however, it's the language we're stuck with, at least for now. Applying the property metaphor to personal information would invariably bring with it a lot of intellectual property's unintended and dangerous baggage—baggage packed for us by the content industries.

The linguistic mess of IP law has already infected the privacy debate. Some users are adamant that they "own their own information," as if they had a natural right to go into every data center in the world and collect a piece of magnetic medium which had somehow been stolen from them by evil corporate pirates. It makes as little sense in the context of personal information as it does in the world of copyrights (where the piracy runs the other way). The metaphor, for better or worse, has been thoroughly corrupted.

Perhaps it will be rehabilitated as we move to a truly digital economy, where physical media is relegated to the world of nostalgia and collectibles. Ownership of copies will give way as the metaphor of content experience to rental, leasing, or use-based pricing.[86] (Think of the success Apple has had with iTunes and, more recently, the iCloud—"the new way to store and access your content.")

Or perhaps we'll continue to get most everything we value for free in exchange for various old and new forms of advertising, some contextual; some product placement; some, well, who knows what the future of advertising will bring? That is, assuming we don't strangle it in its cradle with panicked legislation.

A Better Solution: Licensing Personal Information

The privacy-as-property metaphor is a bad way to transform the property debate from the emotional excesses of the creepy factor into something rational and therefore actually debatable. But there's still hope. For the ownership model isn't that far from something that could prove useful. While intangible property can't be "owned" or "stolen," it can be licensed for particular and limited uses. Personal information, in other words, could be traded in markets that deal not in transfers of ownership but in licenses for use, including leases, rentals, and barters.

Though property and licensing are closely related, licensing has proven to be a much more flexible legal and economic system for dealing with intangibles. When you buy a ticket to a movie theater or a ski lift ticket, the seller isn't transferring ownership of the seat or the gondola, or even a partial or shared transfer of title. You're acquiring a right to use someone else's property, under terms and conditions specified in tiny type but more than likely established by custom and the desire of both parties to have an ongoing, mutually beneficial relationship.

The main advantage of a licensing model is that, unlike the transfer of property rights, there's no need for the transaction to specifically identify the property or to ensure the chain of legal title to it. There's no need to transfer possession of something that, in the case of information, can't be possessed. Licensing is simply permission to use, as general or as specific as the parties decide. The existential nature of the thing being used needn't be determined for licensing to work.

Licensing is the perfect model for information transactions, and it has already been used successfully for many different kinds of information products and services. Your cable provider doesn't own the shows it distributes. Rather, it licenses programming from producers and in turn licenses it to you to watch on authorized devices. Software has moved almost entirely away from the "purchase" of copies of programs on a set of disks to a license to download and execute, or, in the cloud, simply a license to use.[87] Software from Google and other Web-based service providers has always been available to users on a licensed basis, even though the user in most cases pays for the license not with cash but with agreements to share and receive information.

Even when you buy physical copies of information products, you aren't buying the information. Paying for that boxed set of *The Lord of the Rings* movies on extended edition blu-rays, for example, actually encompasses two very different transactions. You own the box, the enclosures, and the DVDs themselves, but you only license the data contained on the disks. The license can be limited (no public showings) or even terminated (watch for 30 days only), which may sound unfair from a property mindset but actually makes possible a wide range of different kinds of transactions, each priced accordingly.

Owners of Amazon Kindles may still talk of "buying" copies of the books they want to read, but the content is mostly in the cloud, available on demand through the Internet. So the terminology is wrong—Kindle readers are actually licensing the future right to read the book. They are paying for permission to use information, not to own or even possess a copy of it.

Proprietary databases, including those from Lexis, West, BNA, and other publishers, are also offered on use-based terms—so much time, or so many users, or both. And more and more application software—whether large corporate systems such as Salesforce.com or the billions of apps downloaded to smartphones and pad computers—is made available on a purely licensed basis.

That transformation, made possible by the Internet, is a boon to consumers. As Kevin Kelly argued in an influential 2009 essay, licensing information use is superior to owning copies of physical media. Physical media takes up space, gets lost, decays or can be damaged. Newer formats often improve on storage capacity, fidelity, and other features and functions.

> There are fewer and fewer reasons to own, or even possess anything. Via [the Internet], the most ordinary citizen can get hold of a good or service as fast as possessing it. The quality of the good is equal to what you can own, and in some cases getting hold of it may be faster than finding it on your own, in your own "basement."[88]

If only we can get past our 20th century prejudice of judging personal worth on the basis of accumulated wealth ("having the most toys"), we can experience the liberation of instant access to the entire corpus of music, film, literature, and services at our fingertips. Licensing rather than possessing copies also means we don't have to store it, clean it, maintain it, or update it when newer and better forms of storage or playback are developed. We might be on our way to information Valhalla. As Kelly says, "Access is so superior to ownership, or possession, that it will drive the emerging intangible economy."[89]

That, in any case, is one possible future for creative content. "Our" "personal" information is evolving to follow the same model, with the dynamics largely reversed. Instead of leasing information from providers, users are increasingly licensing information to them—demographic, transactional, preferences, intimate—in exchange for some kind of valuable service. In the market for personal information, it could be that truly valuable data is exchanged for cash (or coupons), but more likely we'll continue our wildly successful barter system, where information is exchanged for other information—for access to information services that are optimized and customized to our needs and preferences.

How does that market work? The key is the potential of network effects. Remember that intangible goods are different from their physical counterparts in that recombination and reuse make them more valuable rather than using them up. Your personal information may be valuable to you in some abstract sense, but it's really only valuable to others when it can be combined, compared, and repackaged with similar information from other providers.

My purchase history is interesting to my credit card bank because they can use it to figure out what other stuff I might want to buy and what it will take to get me to buy it. But it's really only useful as a network good when it

Your personal information may be valuable to you in some abstract sense, but it's really only valuable to others when it can be combined, compared, and repackaged.

can be combined with the preferences and history of like-minded purchasers. Then it can be used as bargaining leverage with sellers to get volume discounts or to convince them they're making the wrong stuff, in the wrong place, at the wrong price, or at the wrong times.

Purchase information also becomes more valuable, perhaps by orders of magnitude, when transaction information can be combined with information about my experience of the transaction. Did I like the product? How quickly did I use it? What did I use it with? Why did I throw it away? What features actually mattered in my decision to buy, and did those features turn out to be the ones I valued? That kind of post-transaction, subjective, and indeed private information (most of it is currently stuck in my head) can't be easily collected without my cooperation. And that gives me bargaining leverage—an information advantage.

In the past, you have likely used supermarket and other loyalty cards, which trade specific purchase data of a specific customer at a specific store and time for targeted discounts. That's a great example of mutually beneficial information licensing in action. It doesn't matter who "owned" the information, or even whether possessions changed hands. It was a joint creation in which one of the creators (the consumer) authorized the other (the store) to make specified uses of new information.

Let me give two other examples of this barter system now in use. One is the new idea of social shopping, where companies including Groupon and LivingSocial combine the buying preferences of multiple users in a local market. The combined preference information is used to convince a local provider of goods or services that there are new customers who could be acquired if only the right introductory offer is made at the right price and time. If enough users agree to eat at the new sushi restaurant, then it's worthwhile for the sushi restaurant to give us all a healthy discount on a meal, in hopes that many of us will make return visits at full price.

The offline version of that relationship includes buying groups such as Costco and Sam's Club. Members pay an annual fee—the price for the organizer to run the club. The more members, the easier it is to extract high-volume discounts from manufacturers. The more consumers the club can sign up, in other words, the more transactional information the organizers can collect, which they employ as leverage with manufacturers. That's the same kind of network effect that makes the Internet more useful as more people take advantage of it.

To reach the members of the club, in turn, the manufacturers produce special versions of their products (usually the regular products in larger-sized containers, which are cheaper to distribute) and sell them directly to the buying club. The manufacturers avoid several layers of middlemen (so do the buyers), and the extra-large sizes helps allay the complaints of traditional retailers of pricing advantage to the club. In this sense, Costco isn't a store at all; it's a consumer advocacy group, driving hard bargains on behalf of its members. (Priceline works on a similar model.)

The information we give up to participate in these kinds of information barters isn't especially personal, or at least wouldn't be considered so by most users. But what about truly private data? Social networks have already licensed our photos, posts, emails, and other personal content for limited use, mostly to target relevant ads and to help them encourage our friends and family to sign up too.

For the most part, this intimate data isn't being mined all that specifically, at least not so far. Perhaps the providers of these services understand the creepy factor and know that alienating users reverses the value of network effects, which, for social networks, is the beginning of a death spiral. (Just ask the operators of Friendster, MySpace, and other failed social networks. Once networks of any kind stop growing, they quickly begin to shrink.)

The inventory of useful information is about to experience an enormous expansion.

The inventory of useful information, however, is about to experience an enormous expansion, adding leverage for consumers in the information licensing market. Moore's Law, again, is the driver. Now that governments, businesses, and individuals are all on the In-

ternet, we're on the verge of moving to the next level of granularity. It's now cost-effective not just for individuals to have multiple computing devices, but for all the things we interact with to have connectivity as well.

This "Internet of things" will introduce modest processing, storage, and communications technology into each of over a trillion items in commercial use, allowing them to collect and transmit basic information about where they are and what they're doing. Our phones and other mobile devices, including cars, already participate in the Internet of things. Soon it will be appliances, furniture, livestock, light bulbs, fruits and vegetables, and pills.

How does the Internet of things work? In the archetypal example, a radio frequency ID tag is printed onto the packaging of each item—for example, a quart of milk). The tag transmits information about itself whenever it comes near a reader, sometimes operating on static electricity as the power source. The tag helps the store keep track of its inventory and impending expiration dates, and allows you to check out simply by walking past a reader at the exit. Once you're home, the milk, perhaps using the refrigerator as its server, can keep track of usage history and spoilage, letting you know when it's time to restock.

If we allow it, the milk can also pass its status updates (nanotweets?) up the supply chain, giving producers, distributors, retailers, and inspectors consolidated data of tremendous value. Instead of guessing at supply and demand, we'd actually know it. Manufacturing, marketing, pricing and promotion, product design, inventory control, and pretty much every other feature of the industrial economy would become far more efficient—in some cases, for the first time, genuinely scientific.[90]

This coming revolution underscores a feature of privacy that nearly everyone in the discussion today underestimates: The truly valuable uses of information in the future cannot be realized without deep cooperation and collaboration with users. A bank can collect transaction information and public records and create a credit score, but a bank cannot determine how you value your money without your participation. Product marketers can hold focus groups and conduct surveys to determine what to sell and when, but the sample sizes are tiny and unreliable compared to getting actual information from all their customers.

Power is shifting increasingly to users, who will use their digital networks—their social networks, their buying clubs, their email lists, the networks of their possessions—to negotiate for themselves the best possible price for the licensing of information. The need for consumer cooperation and collaboration in future information uses is the best hope for a nonlegislative solution to the privacy problem.

And not just an individual consumer. Nearly all these future information uses are valuable only in large volumes—collecting similar data from everyone. It only matters how well you like a particular product if the retail supply chain can aggregate that information with many other users. That's because intimate information is idiosyncratic, and not highly valued on its own. It is of little interest to any information user except those whose purpose is entirely destructive (e.g., blackmail). In that sense "private" information may come to be defined as information for which there is no market. It's worthless to anyone but the one person who values it exorbitantly.

The expanding market for information licensing, then, may solve the privacy crisis on its own, no new regulation or legislation required. Which is not to say the existing market for information licensing is working perfectly. There are many ways it needs to be improved. Here are some of the most pressing:

1. *Embrace meaningful disclosure*—Service providers must make as clear as possible what information is being collected and what they do with it. This doesn't mean more laws calling for "notice" or "transparency," which generally lead to volumes of disclosures so detailed and technical that any actual important information gets lost. Even a simple mortgage refinance includes over a hundred pages of densely worded disclosures mandated by perhaps a dozen different

The need for consumer cooperation and collaboration in future information uses is the best hope for a nonlegislative solution to the privacy problem.

federal, state, and local agencies. There may be some important information hiding in that mess, but absolutely no one is going to read it all. The more detailed the notice, the less likely it is to communicate anything. Useful disclosures would be short and to the point.[91]

2. *Simplify negotiations*—The higher the transaction costs, the lower the chances of a functioning, efficient market. That's especially true where there are potentially millions of participants and billions of low-value transactions going on all the time. Rather than encouraging information users to negotiate each data element individually (the so-called "opt in" model that some advocates propose, even for social networks whose purpose is to share personal information), look for ways to make it easy for users to vote yes or no on the entire slate of data, at least as the default. Similarly, user agreements, which can establish the basic terms for most information exchanges as an ongoing relationship, must be written to be read and understood by someone other than corporate lawyers.
3. *Secure the information*—Information is valuable, so treat it accordingly. Criminals and other destructive users are ramping up their efforts to gain access to and exploit all kinds of information. Governments, businesses, and consumers must each make better use of existing security procedures and technologies, including encryption, anti-malware, and physical security for data centers and devices. Business information users in particular should take seriously the risk that failure to embrace secure information practices, such as the ISO 27000 series of standards, will surely lead to legislative imperatives that will cost more and protect less. Security breaches are often the only reasons regulators can specify in the rush to enact new privacy laws, though the proposed laws rarely have anything to do with improving security.
4. *Improve self-regulatory practices*—For-profit and not-for-profit entities are emerging to validate the information-handling practices of business users. Businesses should support and embrace these initiatives and take seriously the need to display seals of approval and other indicia of compliance. At the same time, self-regulatory organizations must set real standards and enforce them. Consumers should be educated not to engage in information exchanges with users who don't comply with standards.
5. *Avoid crisis-management regulation*—Regulators must resist the siren call of the privacy crisis du jour, littering the law books with specialized statutes aimed at solving short-term technical problems that will have evolved or mutated before the ink is dry. Limited government resources would be better used to enhance public education on information licensing and to teach consumers how to be effective negotiators. Governments should encourage self-regulation on security, disclosure, and other important elements of the information licensing market, and make clear that fair bargains fairly entered into will be enforced, if necessary, through judicial processes.

Most issues of appropriate use and appropriate compensation for consumer information can and will be worked out by the parties.

These problems are both minor and manageable. The best thing that can be said for the licensing model for information—private or otherwise—is that it's already in place and functioning efficiently and effectively. No new laws must be written to create new rights, and no new regulators are necessary to police them. Abuses are likely to come from activities that are already criminal (hacking and identity theft) or from the government itself.

If current practice is any indicator, most issues of appropriate use and appropriate compensation for consumer information can and will be worked out by the parties. Consumers will continue to show more confidence and ability to express their collective will. If we can just control our reactions to the creepy factor and resist the temptation to

call in our industrial-era government regulators, the long-running and unproductive debate over privacy will be replaced by a more concrete conversation about propriety. That is, how will the wealth generated by valuable new uses of data—personal or otherwise—be shared among information producers and information users?

The legal framework needed for that conversation is already in place. We just have to catch up to our technological innovations. We need to evolve from emotional responses to data use to rational decisionmaking. And we need to do it soon.

Notes

1. See http://www.privacyidentityinnovation.com/.

2. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, p. i, www.ftc.gov/os/2010/12/101201privacyreport.pdf.

3. Ibid., pp. 22–38.

4. Ibid, p. i.

5. Al Franken, Senate Judiciary Subcommittee Hearing on Protecting Mobile Privacy, opening statement, May 10, 2011, http://www.franken.senate.gov/?p=hot_topic&id=1496.

6. Ibid.

7. According to Rackspace, the cost of a gigabyte of storage plummeted from nearly $20 in 2001 to only six cents by 2010. As technology costs decline, new cloud-based services are offering free or extremely cheap virtual storage services for individuals and corporate users, making their money on supplemental services. In 2011 alone, 1.8 zettabytes of new data were created, and projections are that the number of data storage servers will grow 10 times over the next decade. See "Decade of Storage from USB to Cloud Storage," *Rackspace.com* (blog), http://www.rackspace.com/blog/decade-of-storage-from-usb-to-cloud/; and Lucas Mearian, "World Data Will Grow by 50X in next Decade, IDC Study Predicts," *Computerworld*, June 28, 2011, http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X _in_next_decade_IDC_study_predicts.

8. "200 Million Tweets Per Day," Twitter Blog (June 30, 2011), http://blog.twitter.com/2011/06/200-million-tweets-per-day.html.

9. Facebook, "Statistics," http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

10. In 2004, for example, the Electronic Privacy Information Center (EPIC), Privacy Rights Clearinghouse, and the World Privacy Forum sought to have Gmail declared a violation of California wiretapping law. Letter to California Attorney General Bill Lockyer, May 3, 2004, http://epic.org/privacy/gmail/agltr5.3.04.html. At a July 2012 conference, EPIC's executive director confirmed he continued to believe Gmail should be banned. See Berin Szoka, "Video of the Great Privacy Debate Now Available," August 7, 2012, http://techfreedom.org/blog/2012/08/07/video-great-privacy-debate-now-available.

11. "Do Not Track," described as some kind of functional equivalent to telephone "Do Not Call" lists, was a key recommendation in Federal Trade Commission, p. v, 3–4, 13, 28. Details are sketchy, however, as to what exactly is meant by "tracking."

12. Internet Advertising Bureau, "Internet Ad Revenues Hit $31 Billion in 2011, Historic High up 22% over 2010 Record-Breaking Numbers," April 18, 2012, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041812; Adam Thierer, "Birth of the Privacy Tax," *Forbes*, April 4, 2011, http://www.forbes.com/2011/04/02/privacy-tax-social-networking-advertising-opinions-contributors-adam-thierer.html.

13. Google 2012 Financial Tables, http://investor.google.com/financial/tables.html.

14. Lisa Stauber, "A Brief History of Television Advertising," *Television Blend*, Oct. 16, 2006, http://www.cinemablend.com/television/A-Brief-History-of-TV-Advertising-1298.html; Adam Thierer, "We All Hate Advertising, but We Can't Live Without It," *Forbes*, May 13, 2012, http://www.forbes.com/sites/adamthierer/2012/05/13/we-all-hate-advertising-but-we-cant-live-without-it/.

15. We're speaking here of traditional cookies. Flash or "supercookies" are more complicated. See "Cookie Respawning, History Case Dropped," *The Register*, Aug 22, 2011, http://www.theregister.co.uk/2011/08/22/privacy_charge_dropped_against_cookie_trackers/.

16. See Howard Beales, "The Value of Behavioral Targeting," 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. According to Beales's empirical study, conversion rates for behaviorally targeted ads are double the rates for general ads (p. 4).

17. "Half the money I spend on advertising is wasted; the trouble is I don't know which half." At-

tributed to John Wanamaker, see http://www.quotationspage.com/quote/1992.html.

18. See Larry Popelka, "For Successful Innovation, Sell Imperfect Products," *Bloomberg BusinessWeek*, January 25, 2012, http://www.businessweek.com/innovation/for-successful-innovation-sell-imperfect-products-01252012.html.

19. Arthur C. Clarke, *Profiles of the Future: An Inquiry into the Limits of the Possible* (New York: Harper and Row, 1962).

20. Larry Downes, "Privacy Panic Debate: Whose Data Is It, Anyway?", *CNET News.com*, April 27, 2011, http://news.cnet.com/8301-13578_3-20057682-38.html?tag=mncol;1n.

21. See "Geotracking Controversy Homes in on iPhone," *CNET News.com*, July 14, 2011, http://news.cnet.com/8301-13579_3-20057175-37/geotracking-controversy-homes-in-on-iphone-roundup/.

22. Tanzina Vega, "Congress Hears from Apple and Google on Privacy," *New York Times*, May 10, 2011, http://mediadecoder.blogs.nytimes.com/2011/05/10/congress-hears-from-apple-and-google-on-privacy/.

23. "Are your Gadgets Spying on You?" *NPR Science Friday*, May 6, 2011, http://www.npr.org/2011/05/06/136057336/are-your-gadgets-spying-on-you.

24. Brian X. Chen, "U.S. Senator Demands Privacy Policies for Smartphone Apps," *Wired*, May 27, 2011, http://www.wired.com/business/2011/05/u-s-senator-demands-privacy-policies-for-smartphone-apps/.

25. Marguerite Reardon, "Apple: We'll Fix iPhone Tracking 'Bug,'" *CNET News.com*, April 27, 2011, http://news.cnet.com/8301-30686_3-20057815-266.html.

26. "Apple Q&A on Location Data," Apple Press Info, April 27, 2011, http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html.

27. Ibid.

28. "Are Your Gadgets Spying on You?" *NPR Science Friday.*

29. Ibid.

30. William A. Niskanen Jr., *Bureaucracy Public Economics*, 2nd ed. (Northampton, MA: Edward Elgar, 1996).

31. Since 1996, for example, the FCC has expanded its requirement that mobile phones automatically provide location information to emergency service providers. See "In the Matter of Amending the Definition of Interconnected VoIP," Notice of Proposed Rulemaking, FCC 11-107 (2011), http://www.fcc.gov/document/amending-definition-interconnected-voip-service-section-93-commissions-rules-wireless-e911-.

32. See Kim Hart, "Yahoo Changes Data-Retention Policy," *Washington Post*, December 17, 2008; Chloe Albanesius, "AT&T Considering Its Behavioral Advertising Options," *PCmag.com*, August 14, 2008, http://www.pcmag.com/article2/0,2817,2328070,00.asp.

33. See John Eggerton, "House Judiciary Debates Data Retention Bill," *Multichannel News,* July 27, 2011, http://www.multichannel.com/article/471608-House_Judiciary_Debates_Data_Retention_Bill.php. The bill's title suggests retained data could only be used to investigate child pornography, but in fact any crime will do. See Mark Stanley, "How the Data Retention Bill Impacts You," Center for Democracy and Technology, February 27, 2012, https://www.cdt.org/blogs/mark-stanley/2702how-data-retention-bill-impacts-you-%E2%80%93-and-what-you-can-do-about-it; H.R. 1981, "Protecting Children from Online Pornographers Act of 2011," 112th Cong. http://www.govtrack.us/congress/bills/112/hr1981/text.

34. Hart.

35. Amy Lee, "Yahoo Extends Data Retention from 90 Days to 18 Months," *Huffington Post*, April 18, 2011, http://www.huffingtonpost.com/2011/04/18/yahoo-data-retention_n_850373.html.

36. See Henry D. and Frances T. McCallum, *The Wire That Fenced the West* (Norman, OK: University of Oklahoma Press, 1965).

37. Leonard J. Arrington, *The Great Basin Kingdom* (Cambridge: Harvard University Press, 1958).

38. Nathaniel Hawthorne, *The Scarlet Letter* (Boston: Ticknor, Reed, and Fields, 1850).

39. Arrington.

40. Frederick Jackson Turner, "The Significance of the Frontier in American History," in *The Frontier in American History* (New York: Holt, 1920).

41. Jim Harper refers to this as "practical obscurity." See Jim Harper, *Identity Crisis: How Identification Is Overused and Misunderstood* (Washington: Cato Institute, 2006), pp. 158–75.

42. Steven D. Levitt and Stephen J. Dubner, *Super-*

freakonomics (New York: William Morrow, 2011), pp. 139–190.

43. Joseph Heller, *Something Happened* (New York: Alfred A. Knopf, 1974), pp. 13–14.

44. Max Weber, *The Protestant Ethic and the Spirit of Capitalism* (New York: Scribner's, 1958). Weber argued that the "this-worldly asceticism" of Puritanism, encapsulated in the concept of a "calling," drove the development of capitalism and entrepreneurship in Western civilization.

45. European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," COM(2010) 609 (2010). See Larry Downes, "My Own Private Memory Hole," *CNET News.com*, November 16, 2010, http://news.cnet.com/8301-13578_3-20022977-38.html; "US Lobbyists Face Off with EU on Data Privacy Proposal," *Spiegel Online*, October 17, 2012, http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html.

46. U.S. Const. amend. IV.

47. U.S. Const. amend. I.

48. See generally Allison Cerra and Christina James, "Identity Shift" (Cleveland: Wiley, 2012). There is also mounting evidence casting doubt on the value of many of the surveys conducted or financed by self-styled consumer advocates. See Daniel Castro, "New Survey Shows Some Privacy Scholars Lack Objectivity," The Innovation Files, Oct. 14, 2012, http://www.innovationfiles.org/new-survey-shows-some-privacy-scholars-lack-objectivity/.

49. Warren and Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 193 (1890). ("Of the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency.") Warren, married to the daughter of a U.S. Senator, was motivated in part by outrage when trivial details of a social function attended by his daughter were mentioned in the *Washington Post*. Like today's social networks, photography came with both costs and benefits to social and family life.

50. For the development and decline of common law privacy torts, see *Haynes v. Knopf*, 8 F3d. 1222 (7th Cir. 1993) (Posner).

51. Warren and Brandeis.

52. Federal Trade Commission, p. vi.

53. Sean Ludwig, "LinkedIn Removes Photos from 'Social Ads' after Complaints," VentureBeat, August 11, 2011, http://venturebeat.com/2011/08/11/linkedin-social-ads-pictures-removed/.

54. Ryan Roslansky, LinkedIn Blog, August 11, 2011, http://blog.linkedin.com/2011/08/11/social- ads-update/.

55. Eric Goldman, "Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts," *Forbes.com*, September 28, 2012, http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/.

56. See http://online.wsj.com/public/page/what-they-know-digital-privacy.html. The *New York Times* is also getting into the fear-mongering business. See Natasha Singer, "Consumer Data, but Not for Consumers," *New York Times*, July 21, 2012, http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all; Natasha Singer, "You for Sale: Mapping, and Sharing, the Consumer Genome,"*New York Times*, July 16, 2012, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all ("In essence, it's as if the ore of our data-driven lives were being mined, refined, and sold to the highest bidder, usually without our knowledge—by companies that most people rarely even know exist"); Natasha Singer, "Do Not Track? Advertisers Say 'Don't Tread on Us,'" *New York Times*, October 13, 2012, http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html ("But what is really at stake here is the future of the surveillance economy").

57. Julia Angwin, "The Web's New Gold Mine: Your Personal Secrets," *Wall Street Journal*, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

58. See Jim Harper, "Schneier on RealAge.com: Factually Incorrect," *Technology Liberation Front*, April 28, 2009, http://techliberation.com/2009/04/28/schneier-on-realage com-factually-incorrect/.

59. The European Union issued a directive in 2011 that requires explicit consent to place a cookie on a user's computer, but the directive has proven difficult to translate into enforceable regulation. See "Will UK.gov Crack Down on Itself for Missing Cookie Law Deadline?" *The Register*, May 18, 2012, http://www.theregister.co.uk/2012/05/18/most_gov_websites_will_miss_cookies_law_deadline/.

60. Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964).

61. The Privacy Act of 1974, Pub.L. 93-579 (1974). For recent interpretation, see *FAA v. Cooper*, 131 S.Ct. 3025 (2012). Cooper sued the government when Social Security Administration personnel revealed details of his health status to the Federal Aviation Administration, where he was licensed as a pilot.

62. Or worse, so general as to be serviceable by any ambitious agency or prosecutor eager to fit high creepy factor activities that were clearly not in the minds of those who voted for the legislation. A good example is the Computer Fraud and Abuse Act, 18 U.S.C. §1030, which prosecutors have tried—ultimately without success—to use in place of nonexistent laws against cyberbullying and employee appropriation of company data. See Larry Downes, "Lori Drew Verdict Finally Overturned," Stanford Center for Internet and Society, August 31, 2009, http://cyberlaw.stanford.edu/node/6246, and "US will not Challenge Computer Fraud Case to High Court, *NBC News.com*, August 9, 2012, http://www.technolog.msnbc.msn.com/technology/technolog/us-will-not-challenge-computer-fraud-case-high-court-932764.

63. Sheldon Richman, "Dissolving the Inkblot: Privacy as Property Right," *Cato Policy Report* 15, no. 1 (1993).

64. Lawrence Lessig, "Privacy as Property," *Social Research* 69, no. 1 (2002).

65. Ibid.

66. See Larry Downes, *The Laws of Disruption* (New York: Basic Books, 2009), chap. 2, "The Weird Economics of Information," pp. 25–44.

67. According to the Pew Internet and American Life Project, "Two-thirds of those who download music files or share files online say they don't care whether the files are copyrighted or not." Amanda Lenhart and Mary Madden, "Music Downloading, File-Sharing, and Copyright," Pew Internet and American Life, 2003, http://www.pewinternet.org/Reports/2003/Music-Downloading-Filesharing-and-Copyright/Data-Memo.aspx.

68. See Richard A. Posner, "Why There Are Too Many Patents in America," *The Atlantic*, July 12, 2012, http://www.theatlantic.com/business/archive/2012/07/why-there-are-too-many-patents-in-america/259725/.

69. R. H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3, no.1 (1960).

70. R. H. Coase, "The Nature of the Firm," *Economica* 4, no. 16, (November 1937): 386–405.

71. See, for example, Jeff Gelles, "Verizon Wireless Policy Change Raises Privacy Issues," *Philadelphia Enquirer,* October 20, 2011, http://articles.philly.com/2011-10-20/business/30301830_1_verizon-and-verizon-wireless-privacy-policy-new-advertising-program.

72. *See* Cal. Civ. Code §3344 (1984); NY CLS Civ. R. § 50 (2000).

73. *Haynes v. Knopf*.

74. Nicholas Lemann, *The Promised Land: The Great Black Migration and How it Changed America* (New York: Vintage, 1991).

75. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

76. The case might have had a different outcome in the European Union, which is working out the specifics of a "right to be forgotten," which EU regulators see as a natural extension of the EU's more abstract privacy directives. See Larry Downes, "My Own Private Memory Hole," *CNET News.com*, November 16, 2010, http://news.cnet.com/8301-13578_3-20022977-38.html.

77. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

78. There are similar examples of laws regulating private sector use of information in health care, lending, mortgages, and laws that prohibit discrimination in housing, lending, insurance, and employment based on specific data such as age, race, ethnicity, gender, and other characteristics long associated with irrational prejudices. Which ones satisfy the criteria described above and which were necessitated by genuine market failures are questions well outside the scope of this essay.

79. Lessig in fact dodges even further. "The property right I am imagining governs the terms under which one machine can access certain data from the other machine. It says that the party who would collect these facts cannot do so without permission from [my computer]. The default is that the facts cannot be collected, but that default can be negotiated around." It is clear that by "certain data" he means "private" data, but the article never says so explicitly, nor answers the question of how that class of data would be defined.

80. Natasha Singer, "Consumer Data, but Not for Consumers."

81. For origins of the phrase, see R. Polk Wagner, "Information Wants to Be Free: Intellectual Property and the Mythologies of Control," *Columbia Law Review* 103, no. 4 (May 2003): 995–1034.

82. Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964).

83. See F. Gregory Lastowka and Dan Hunter, "Amateur-to-Amateur: The Rise of a New Creative Culture," Cato Policy Analysis no. 567, April 26, 2006 http://www.cato.org/publications/policy-analysis/amateuramateur-rise-new-creative-culture.

84. The RIAA has been pursuing its sole litigated case since 2008 against Jammie Thomas-Rasset, who was found to have shared 24 songs without authorization, leading to statutory damages of $1.5 million. The case has become a public relations nightmare for the industry. See Greg Sandoval, "RIAA Files Appeal in Jammie Thomas Case," *CNET News.com*, August 22, 2011, http://news.cnet.com/8301-31001_3-20095566-261/riaa-files-appeal-in-jammie-thomas-case/.

85. Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," *Wall Street Journal*, December 19, 2008, http://online.wsj.com/article/SB122966038836021137.html.

86. Kevin Kelly, "Better than Owning," *The Technium*, January 21, 2009, http://www.kk.org/thetechnium/archives/2009/01/better_than_own.php.

87. Larry Downes, "The End of Software Ownership—and Why to Smile," *CNET News.com*, September 20, 2010, http://news.cnet.com/8301-1001_3-20016 864-92.html.

88. Kelly.

89. Ibid.

90. See generally "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, 2011, http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation.

91. This is especially important for mobile apps, where screen real estate is limited and the ability to convey detailed information is constrained even further. See Tanzina Vega, "Industry Tries to Streamline Privacy Policies for Mobile Uses," *New York Times*, August 14, 2011.

RELATED PUBLICATIONS FROM THE CATO INSTITUTE

Reputation under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate by Jim Harper, Cato Institute Policy Analysis no. 690 (December 8, 2011)

Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration by Jim Harper, Cato Institute Policy Analysis no. 612 (March 6, 2008)

Amateur-to-Amateur: The Rise of a New Creative Culture by F. Gregory Lastowka and Dan Hunter, Cato Institute Policy Analysis no. 567 (April 26, 2006)

Understanding Privacy—and the Real Threats to It by Jim Harper, Cato Institute Policy Analysis no. 520 (August 4, 2004)

Human Bar Code: Monitoring Biometric Technologies in a Free Society by F. Gregory Lastowka and Dan Hunter, Cato Institute Policy Analysis no. 452 (September 17, 2002)

Internet Privacy and Self-Regulation: Lessons from the Porn Wars by Tom W. Bell, Cato Institute Briefing Paper no. 65 (August 9, 2001)

Capital Markets: The Rule of Law and Regulatory Reform by Solveig Singleton, Cato Institute White Paper (September 13, 1999)

RECENT STUDIES IN THE CATO INSTITUTE POLICY ANALYSIS SERIES

715. **Humanity Unbound: How Fossil Fuels Saved Humanity from Nature and Nature from Humanity** by Indur M. Goklany (December 20, 2012)

714. **On the Limits of Federal Supremacy: When States Relax (or Abandon) Marijuana Bans** by Robert A. Mikos (December 12, 2012)

713. **India and the United States: How Individuals and Corporations Have Driven Indo-U.S. Relations** by Swaminathan S. Anklesaria Aiyar (December 11, 2012)

712. **Stopping the Runaway Train: The Case for Privatizing Amtrak** by Randal O'Toole (November 13, 2012)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30-4:30 eastern time). Fax (202) 842-3490 • www.cato.org

Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You

Eugene Volokh*

Proposed "information privacy" rules that give us the power to "control ... information about ourselves" sound undeniably appealing. The First Amendment, however, generally bars the government from "control[ling the communication] of information," either by direct regulation or through the authorization of private lawsuits. This article argues that: (1) While privacy protection secured by contract turns out to be constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law. (2) Creating new free speech exceptions to accommodate information privacy speech restrictions could have many unfortunate and unforeseen consequences. Most of the justifications given for information privacy speech restraints are directly applicable to other speech control proposals that have already been suggested, and accepting these justifications in the attractive case of information privacy speech restrictions would create a powerful precedent for those other restraints.

* Professor of Law, UCLA Law School (volokh@law.ucla.edu). Many thanks to Stuart Benjamin, Jerry Kang, Marty Lederman, Michael Madison, Dawn Nunziato, and Malla Pollack for their very helpful advice. Thanks also to Paul Schwartz for his thoughtful, gracious, and generous commentary on this piece, Paul M. Schwartz, *Free Speech vs. Information Privacy*, 52 STAN. L. REV. 1559 (2000).

INTRODUCTION

Privacy is a popular word, and government attempts to "protect our privacy" are easy to endorse. Government attempts to let us "control . . . information about ourselves"[1] sound equally good: Who wouldn't want extra control? And what fair-minded person could oppose requirements of "fair information practices"?[2]

The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is

1. Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) (a classic in the field); *see also, e.g.*, Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1155 (1997); Berman & Mulligan, *infra* note 36, at 575; Shorr, *infra* note 98, at 1767.

2. *See, e.g.*, Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995).

a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits[3]), whether the communication is "fair" or not.[4] While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.

Of course, the Supreme Court and even lower courts can create new First Amendment exceptions or broaden existing ones; and if the courts did this for information privacy speech restrictions, . can't say that I'd be terribly upset about the new exception for its own sake. Speech restrictions aimed at protecting individual privacy just don't get my blood boiling. Maybe they should, but they don't. Perhaps this is because, from a selfish perspective, I'd like the ability to stop others from talking about me, and while I wouldn't like their stopping *me* from talking about *them,* the trade-off might be worth it.

Nonetheless, I'm deeply worried about the possible downstream effects of any such new exception. Most of the justifications given for information privacy speech restraints are directly applicable to other speech controls that have already been proposed. If these justifications are accepted in the attractive case of information privacy speech restrictions, such a decision will be a powerful precedent for those other restraints and for still more that might be proposed in the future.

Thus, for instance, some argue that information privacy laws are defensible because they protect an intellectual property right in one's personal information.[5] Such arguments don't fit well into the intellectual property exceptions to the First Amendment, which generally don't entitle anyone to restrict the communication of facts. And if we are to consider extending the existing exceptions, we should also consider that an intellectual property rights rationale is already being used as an argument for other speech restrictions: the proposed database protection law, the attempts to expand the right of publicity, and more. Before wholeheartedly endorsing the principle that calling certain information "intellectual property" lets the government restrict speech communicating that information, we should think about the consequences of such an endorsement.

---

3. *Cf., e.g.*, New York Times v. Sullivan, 376 U.S. 254, 265 (1964) (holding that the First Amendment applies to "civil lawsuit[s] between private parties," because such lawsuits involve "[state] courts . . . appl[ying] a state rule of law").

4. If "fair information practices" applied only to the government's control of its own speech, I would have had no objection to them. *See infra* Part I. But governmental restriction of supposedly "unfair" speech by nongovernmental entities raises serious First Amendment problems.

5. *See infra* Part III.

Similar problems confront the arguments that information privacy speech restrictions are constitutional because they restrain only commercial speech,[6] restrain only speech that is not on matters of public concern,[7] are narrowly tailored to a compelling government interest in protecting people's dignity, emotional tranquility, or safety,[8] are needed to protect a countervailing civil right,[9] or pass muster under a "context-sensitive balancing."[10] First, for these arguments to succeed, existing First Amendment precedents would have to be substantially stretched. Second, the stretching may make the doctrine loose enough to give new support to many other restrictions. Bans on sexually themed speech might become justified under a "no public concern" rationale. Campus speech codes might be justified under a "countervailing civil right" rationale or a "narrowly tailored to a compelling government interest" rationale. Restrictions on online discussion about economic matters or on consumer complaints might be justified under a broadened commercial speech rationale. Restrictions on online distribution of information about encryption or drugs might be justified under a crime prevention rationale. And who knows what might be allowed under "context-sensitive balancing," which has in practice long been a tool for judges to justify a wide range of speech restrictions?

In making these arguments, I will try to identify concrete, specific ways—doctrinal, political, and psychological—in which upholding certain kinds of information privacy speech restrictions could affect the protection of other speech. I will try to avoid making general slippery slope arguments of the "today this speech restriction, tomorrow the Inquisition" variety; the recognition of one free speech exception certainly does not mean the end of free speech generally, or else all would have been lost long ago. But slippery slope concerns are still quite sensible, especially when accepting a proposed speech restriction entails accepting a principle that is broader than the particular proposal and that can logically cover many other kinds of restraints.[11]

---

6. *See infra* Part IV.

7. *See infra* Part V.

8. *See infra* Part VI.

9. *Id.*

10. Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1422 (2000).

11. *See* text accompanying notes 182 and 183 *infra*. One of the most eloquent American expressions of this concern with uncabinable principles is also among the earliest:

> [I]t is proper to take alarm at the first experiment on our liberties. We hold this prudent jealousy to be the first duty of citizens, and one of [the] noblest characteristics of the late Revolution. The freemen of America did not wait till usurped power had strengthened itself by exercise, and entangled the question in precedents. They saw all the consequences in the principle, and they avoided the consequences by denying the principle. We revere this lesson too much, soon to forget it. Who does not see that the same authority which can establish Christianity, in exclusion of all other Religions, may establish with the same ease any particular sect of Christians, in exclusion of all other Sects? That the same authority which can force a citizen

Our legal system is based on precedent. Our political life is in large measure influenced by arguments by analogy. And many people's normative views of free speech are affected by what courts say: If the legal system accepts the propriety of laws mandating "fair information practices," people may becomes more sympathetic to legal mandates of, for instance, fair news reporting practices or fair political debate practices.[12]

This article is an attempt to consider, as concretely as possible, the possible unintended consequences of various justifications for information privacy speech restrictions. I ultimately conclude that these consequences are sufficiently troubling that I must reluctantly oppose such information privacy rules. But I hope the article will also be useful to those who are committed to supporting information privacy speech restrictions, but would like to design their arguments in a way that will minimize the risks that I identify; and even to those who welcome the possibility that information privacy speech restrictions may become a precedent for other restrictions, because they believe the Court has generally gone too far in protecting, say, nonpolitical speech or speech that injures the dignity of others. Thinking ahead about the possible unintended implications of a proposal—even, and perhaps especially, if it seems viscerally appealing—is always worthwhile.

---

to contribute three pence only of his property for the support of any one establishment, may force him to conform to any other establishment in all cases whatsoever?

James Madison, *Remonstrance Against Religious Assessments* (1786), *quoted in* Everson v. Board of Educ., 330 U.S. 1, 65-66 (1947). I likewise fear that the same authority which can force a citizen to stop speaking on one matter by, for instance, defining it out of the zone of "legitimate public concern" may in time do the same as to speech on other matters.

12. For some examples of past attempts to restrict such "unfair" speech, see, e.g., Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (rejecting attempt to impose liability for a publisher's vicious parody of a political enemy); Miami Herald v. Tornillo, 418 U.S. 241 (1974) (rejecting attempt to require a newspaper to publish rebuttals of attacks on a consolidate); Keefe v. Organization for a Better Austin, 402 U.S. 415 (1971) (rejecting attempt to enjoin leafletting aimed at pressuring a local resident to change his business practices); Mills v. Alabama, 384 U.S. 214 (1966) (rejecting attempt to ban election-day political editorials in the interests of preventing unrebuttable attacks).

The European Personal Data Directive, which is often praised by privacy advocates, does require countries to create a code of fair news reporting practices: It on its face applies to journalism that reveals personal data such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," and mandates that governments create exemptions for journalism, art, or literature "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." Directive 95/46/EC, 1995 O.J. (L 281) 31, arts. 8(1), 9. What this provision will ultimately mean is so far unclear. *Cf.* James R. Maxeiner, *Freedom of Information and the EU Data Protection Directive*, 48 FED. COMM. L.J. 93, 102 (1995) (stating that the "only if they are necessary" language was added to prevent "the balance [from] fall[ing] too much in favor of the media," and concluding that the scope of the journalism exception is uncertain); Paul Eastham, *I Would Have Gagged the Press Over Cook*, LONDON DAILY MAIL, Feb. 5, 1998, at 2 (quoting the senior English Law Lord as taking the view that the privacy directive would have barred certain news stories about a cabinet minister's alleged affair).

The disclosure tort, of course, has always been an attempt to mandate fair news reporting practices.

I. INFORMATION PRIVACY SPEECH RESTRICTIONS

My analysis throughout this article will focus on the government acting as sovereign, restricting what information nongovernmental speakers may communicate about people. I thus exclude restrictions that the government imposes on its own agencies, such as Freedom of Information Act provisions that prevent government revelation of certain data,[13] or IRS or census rules that prohibit the communication of some tax or census data to other government agencies or to the public.[14] Government agencies do not have free speech rights against their own governments; for instance, federal agencies must comply with congressional mandates, and creatures of the state such as city or county governments cannot claim rights against the state legislature.[15] Whether speech by state agencies may be restrained by the federal government is a tougher question, but one that's beyond the scope of this article.[16] By focusing on communication by nongovernmental speakers—reporters, businesspeople, private detectives, neighbors—I limit the inquiry to people and organizations that indubitably have free speech rights.

I also exclude restrictions that the government imposes as an employer (e.g., telling its employees that they may not reveal confidential information learned in the course of employment), or as a contractor putting conditions

---

13. *E.g.*, 5 U.S.C. § 552(b)(6).

14. *E.g.*, 13 U.S.C. § 9(a); 26 U.S.C. § 6103(a). *Cf.* Singleton, *infra* note 251 (arguing for strong restrictions on government collection and communication of personal information); Schwartz, *supra* note *, at 1562 (correctly pointing out that many such "fair information practices" rules are not subject to my analysis).

15. *See, e.g.*, Anderson v. City of Boston, 380 N.E.2d 628, 637 (Mass. 1979).

16. *See* Roderick M. Hills, Jr., *Back to the Future? How the Bill of Rights Might Be About Structure After All*, 93 NW. U. L. REV. 977, 1004 & n.98 (1999) (discussing this issue, and arguing that state and local agencies should have free speech rights against the federal government). Note that *Reno v. Condon*, 120 S. Ct. 666 (2000), which upheld against a Tenth Amendment challenge a federal restraint on state communication of information, did not confront—and thus did not resolve—the First Amendment question. "Cases cannot be read as foreclosing an argument that they never dealt with." Waters v. Churchill, 511 U.S. 661, 678 (1994) (plurality opinion) (citing United States v. L.A. Tucker Truck Lines, Inc., 344 U.S. 33, 38 (1952)); *see also* Miller v. California Pac. Med. Ctr., 991 F.2d 536, 541 (9th Cir. 1993) ("It is a venerable principle that a court isn't bound by a prior decision that failed to consider an argument or issue the later court finds persuasive."); *cf.* White v. Massachusetts Council of Constr. Employees, 460 U.S. 204 (1983) (holding that preference in city-funded construction contracts for city residents passed muster under the Commerce Clause) and United Bldg. & Constr. Trades Council v. Mayor of Camden, 465 U.S. 208 (1984) (holding that such preferences violated the Privileges and Immunities Clause). And it is not surprising that the Court didn't confront the First Amendment issue; it's standard practice for the Court not to discuss issues (especially complex issues) that weren't raised by the parties in their Supreme Court briefs, or discussed in the lower court opinion. *See, e.g.*, Bankers Life & Cas. Co. v. Crenshaw, 486 U.S. 71, 79 (1988).

The question of what the federal government could do to constrain speech by state agencies that reveals information about people is a genuinely hard question, and I don't know which way the Court will or should come out on it; my only point here is that the question isn't answered by *Condon*.

on the communication of information that it has no constitutional duty to reveal (e.g., telling people who want certain lists from the Federal Election Commission that they may only get them if they promise not to use those lists for certain purposes,[17] or telling litigants that they will get discovery materials only if they promise not to reveal them[18]). The government has long been held to have much broader powers when it's acting as employer or contractor, imposing constraints on those who assume them in exchange for government benefits or for access to government records, than when it's acting as sovereign, controlling the speech of private citizens.[19] The unconstitutional conditions doctrine may impose some limits even on the government acting as employer or as contractor, but I will set these matters aside for purposes of this article.

I also focus only on restrictions on communication. Other things that are often called privacy rules—the right to be free from unreasonable governmental searches and seizures, the right to make certain decisions about one's life without government interference, the right not to have people listen to you or watch you by going onto your property, the right not to have people electronically eavesdrop on your conversations, the requirement that credit bureaus notify consumers when credit reports about them are prepared, and the like—are outside the scope of my discussion.[20] Some of these laws, for instance restraints on government snooping or control, pose no First Amendment problems. For other laws, such as restrictions on nongovernmental gathering of information through nonspeech means, the First Amendment rules are unclear; but it is clear that the analysis of restrictions on information gathering is different from the analysis of restrictions on speech.[21] It is the latter doctrine that is most fully developed, and that provides the most protection against government restrictions.

These three exclusions merely reflect the fact that the strongest protection of free speech has long been seen as arising when the government is acting as sovereign, restricting the speech of private parties. And within this zone lie a variety of current and proposed speech restrictions:

1. The "disclosure" tort, which bars the public dissemination of "nonnewsworthy" personal information that most people would find highly pri-

17. *See, e.g.*, FEC v. International Funding Inst., Inc., 969 F.2d 1110 (D.C. Cir. 1992) (en banc); Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999) (not reaching the merits of the question).

18. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984).

19. *See, e.g.*, Waters v. Churchill, 511 U.S. 661, 671 (1994) (plurality); Rust v. Sullivan, 500 U.S. 173, 193 (1991).

20. *See, e.g.*, Prahl v. Brosamle, 295 N.W.2d 768, 780-81 (Wis. Ct. App. 1980) (holding that the First Amendment doesn't license trespasses committed in the interests of newsgathering).

21. *See, e.g., Seattle Times*, 467 U.S. at 32; Houchins v. KQED, Inc., 438 U.S. 1, 12 (1978) (4-3 decision).

vate,[22] and more specific state laws that forbid some such communications, for instance criminal laws forbidding the publication of the names of rape victims.[23] The uniting principle here is that it is particularly embarrassing to reveal a certain narrow range of information about people, for instance their medical histories, their criminal histories, their sexual practices, the images of their naked bodies, the contents of their conversations with their lawyers or psychiatrists, or possibly some of their reading or viewing habits.[24] These laws generally bar the communication of such information to the public, precisely because it's the publicizing of such potentially embarrassing information—either to large groups of people or possibly to smaller groups (friends, neighbors, and business associates) whose opinion the subject especially values—that is usually seen as especially offensive.

2. Proposed restrictions on communication of all sorts of information about people, including matters that are not generally seen as especially private, for instance the food or clothes they buy, the stores (online or offline) they've shopped at, and so on.[25] Some such information may be embarrassing, but these laws do not focus on that; rather, they cover all information about a person, or at least all information that was gathered in a particular way (for instance, through online business transactions with that person).[26] And because embarrassment isn't the major concern, these laws also apply to communications aimed at fairly narrow groups of recipients about whose opinion most people care little—for instance, communications to another business that wants to sell things to you. The felt injury here is the perceived indignity or intrusion flowing from the very fact that people are talking about you or learning about you, and not the embarrassment flowing from the fact that people are learning things that reflect badly on you.
3. Finally, a narrow range of restrictions aimed at preventing people from communicating information that might put others in danger of crime, for instance (in some contexts) the names of witnesses or jurors,[27] or data-

22. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

23. *See, e.g.*, FLA. STAT. ANN. § 794.03 (West 1987), held unconstitutional by Florida Star v. B.J.F., 491 U.S. 524 (1989).

24. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (barring video stores from communicating information about their customers' rental records).

25. *See, e.g.*, Gindin, *supra* note 1, at 1157 (urging restrictions on communication of "data on neighboring properties, . . . plane and boat ownership, motor vehicle records, voter registration records, law suits, liens and judgments [and] criminal records").

26. *See, e.g., id.* at 1219-22.

27. *See, e.g., infra* note 285.

bases of people's social security numbers that some can use to engage in fraud.[28]

Each of these categories covers some restrictions that are imposed only on the subject's business partners (for instance, bans on lawyers revealing information about their clients, or bans on businesses revealing information about their customers) and other restrictions that are imposed on everyone (for instance, bans on the media publishing embarrassing information that they learned from third parties, or property rights in information that bind everyone without regard to whether they've entered into any contracts). And of course these categories may overlap: Some restrictions aim at preventing embarrassment, preventing crime, and preventing communications about people more broadly.

II. CONTRACT

A. *Permissible Scope*

To begin with, one sort of limited information privacy law—contract law applied to promises not to reveal information[29]—is eminently defensible under existing free speech doctrine. The Supreme Court explicitly held in *Cohen v. Cowles Media* that contracts not to speak are enforceable with no First Amendment problems.[30] Enforcing people's own bargains, the Court concluded (I think correctly), doesn't violate those people's rights, even if they change their minds after the bargain is struck. Some have criticized this conclusion on the grounds that it slights the interests of the prospective listeners, and this criticism has some force. Still, I think that ultimately the free speech right must turn on the rights of the speakers, and that it's proper to let speakers contract away their rights—and certainly this is the view that the *Cohen v. Cowles Media* Court took. Insisting that people honor their bargains is a constitutionally permissible "code of fair practices," whether information practices or otherwise.

And such protection ought not be limited to express contracts, but should also cover implied contracts (though, as will be discussed below, there are

28. *Cf., e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1197 n.12 (1998) (discussing the controversy over Lexis-Nexis's P-Trak database, which allegedly disclosed information that could be used to commit credit card fraud).

29. *See, e.g., id.* at 1268; Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591 (1994).

30. 501 U.S. 663 (1991). The Court also said that the First Amendment allows enforcement of promises which do not constitute contracts, but which are enforceable under the law of promissory estoppel; but any contract law differences between contract and promissory estoppel don't affect the Court's key conclusion, which is that people may promise not to say certain things and thus waive their free speech rights. For convenience, then, I'll talk about this as the "contract" doctrine of First Amendment law.

limits to this theory). In many contexts, people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract[31]—that part of what their contracting partner is promising is confidentiality. This explains much of why it's proper for the government to impose confidentiality requirements on lawyers, doctors, psychotherapists, and others: When these professionals say "I'll be your advisor," they are implicitly promising that they'll be confidential advisors, at least so long as they do not explicitly disclaim any such implicit promise.[32]

Laws that explicitly infer such contracts from transactions in which there's no social convention of confidentiality are somewhat more troublesome, especially if they require relatively formal disclaimers. Imagine, for instance, a law providing that all questions by reporters will be interpreted as implicitly promising not to quote the source by name in a published article, unless the source consents in writing after being given full disclosure of the true purpose for which the quote is to be used. Or consider a law providing that people who buy a product implicitly promise to give the seller equal space to respond to any negative article they publish about the product, unless the seller consents in writing after being given full disclosure of the true purpose for which the product is being bought.[33] Though journalists could avoid the restriction by getting the requisite explicit consent, the request for the consent may deter many of the sources and especially many of the sellers; and this in turn may deter journalists from publishing hostile reviews or stories that include quotes which show the sources in a bad light.

---

31. *See* RESTATEMENT (SECOND) OF CONTRACTS § 4 cmt. a (1979).

32. *See, e.g.*, Geisberger v. Willuhn, 390 N.E.2d 945, 947-48 (Ill. App. Ct. 1979) (physician); Suburban Trust Co. v. Waller, 408 A.2d 758, 762 (Md. Ct. Spec. App. 1979) (bank); Doe v. Roe, 400 N.Y.S.2d 668 (1977) (psychiatrist); Hammonds v. Aetna Cas. & Sur., 243 F. Supp. 793, 801-02 (N.D. Ohio 1965) (physician); Murphy, *infra* note 47, at 2408-10. Some disclosure tort cases, such as *Vassiliades v. Garfinckel's*, 492 A.2d 580 (D.C. 1985), where a plastic surgeon used his patient's before and after pictures without her consent, may have been better analyzed this way.

The approach I outline here is thus in large part, though perhaps not entirely, consistent with suggestions recently made by Jessica Litman and Pam Samuelson. Professor Samuelson would punish unconsensual communication of personal data by merchants under a quasi-trade-secret theory, Samuelson, *infra* note 60, at 1156-57, but she makes clear that her argument rests on *Cohen v. Cowles Media*, *id.* at 1157 n.70, and seemingly would restrict only disclosures by the contracting party. Professor Litman would prohibit such behavior on the grounds that it is a "breach of trust," Litman, *infra* note 60, at 1308, and while she would implement this through a tort regime, I think that a *Cohen v. Cowles Media*-based implied contract theory is the best First Amendment justification for this proposal.

33. These examples may seem unusual, but given current hostility towards perceived media overreaching and the fact that many relatively powerful interests see themselves as victims of out-of-context quotes or unfair product reviews, *see, e.g.*, David J. Bederman, Scott M. Christensen & Scott Dean Quesenberry, *Of Banana Bills and Veggie Hate Crimes: The Constitutionality of Agricultural Disparagement Statutes*, 34 HARV. J. ON LEGIS. 135 (1997), they are hardly inconceivable (though, since the media are also a powerful interest group, the laws I describe wouldn't be shoo-ins, either).

These concerns may justify treating the *Cohen v. Cowles Media* principle as applicable only to those implied contracts where confidentiality really is part of most people's everyday expectations. This would mean the implicit contract theory could uphold laws that by default prevent lawyers, doctors, psychiatrists, sellers of medical supplies, and possibly sellers of videos and books from communicating information about their customers; but it wouldn't uphold laws that by default prevent reporters (who are notorious for communicating embarrassing things, not keeping them confidential) from revealing what was said to them, prevent consumers from reviewing products, or prevent sellers of groceries or shoes from communicating who bought what from them. I doubt that most of us expect that someone selling us our food is implicitly promising to keep quiet about what they sold us.[34]

On the other hand, I'm not sure that such a narrow application of *Cohen v. Cowles Media* is proper or ultimately workable. It's often hard to determine exactly what most people expect. When someone buys a video, especially a video whose title he wouldn't want associated with his name, he probably assumes that the video store won't publicize the purchase, at least in part because a video store that does publicize such purchases would lose a lot of business.[35] But is he assuming that the video store is *promising* not to publicize such a purchase? He probably isn't even thinking about this.[36]

If he is assuming such a promise, is he assuming that the video store is promising not to communicate information about such a purchase at all, or

---

34. Such a view might also be supported by the principle of *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992), which held that the government generally may not discriminate based on content even within a category of unprotected speech; by analogy, one can argue that, even if speech that breaches a contract may be unprotected under *Cohen v. Cowles Media*, the government may not impose default contract conditions in content-based ways or impose different sanctions for breaches of different speech-restrictive contracts. The full scope of *R.A.V.*, though, is not quite clear, in part because of the somewhat mysterious exception for situations where "there is no realistic possibility that official suppression of ideas is afoot." 505 U.S. at 390.

35. Michael Froomkin astutely points out that this is probably one reason why the Video Privacy Protection Act and the similar provisions in the Cable Communications Policy Act of 1984, 47 U.S.C. § 551, have never been challenged on First Amendment grounds: "[M]erchants in these two industries sell a great deal of sexually themed products and have no incentive to do anything that reduces their customers' belief that their viewing habits will not become public knowledge." A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1522 (2000).

36. *Cf., e.g.*, Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 563 (1999) ("When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will base the information collected on the service and use it for the sole purpose of providing the service requested."); Pamela Samuelson, *A New Kind of Privacy?*, 87 CAL. L. REV. 751, 768 (1997) ("[P]olls show that many people who disclose to others information about themselves for a particular purpose (*e.g.*, to get credit or to be treated for a disease) believe that their disclosures have been made under an implied, if not an explicit, pledge to use the data only for that purpose."). I suspect that this is true of doctors, less true of banks, and least true of merchants, especially given people's knowledge that merchants do sell customer information to each other. On the other hand, I also suspect that most people have little expectation about many such transactions—especially transactions with merchants other than doctors and banks—simply because they haven't much thought about the matter.

only promising not to pass it along to the public or his neighbors, while reserving the right to communicate it to others in the same business? Again, most buyers probably have not even thought about the matter. One advantage of statutory default rules is precisely that they clarify people's obligations instead of leaving courts to guess what people likely assumed.

So I tentatively think that a legislature may indeed enact a law stating that certain legislatively identified transactions should be interpreted as implicitly containing a promise of confidentiality, unless such a promise is explicitly and prominently disclaimed by the offeror, and the contract together with the disclaimer is accepted by the offeree.[37] True, this might justify laws that treat reporters as implicitly promising that they won't reveal or even quote their sources, which troubles me. But so long as the implicit promise is genuinely disclaimable, I'm not too troubled. Even if this might eventually lead to the reporter hypothetical, I don't think too much would be lost; and what is gained from allowing statutorily defined default nondisclosure rules is the clear enforceability of promises that often are reasonably inferred by one of the contracting parties, and that can be important parts of the bargain.

Furthermore, though *Cohen v. Cowles Media* involved traditional enforcement of a promise through a civil suit, there should be no constitutional problem with the government enforcing such promises through administrative actions, or using special laws imposing presumed or even punitive damages for breaches of such promises. I suspect that even with purely contractual remedies, the threat of class action suits could be a powerful deterrent to breaches of information privacy contracts by e-commerce sites, especially since the suits would create a scandal: In the highly competitive Internet world, a company could lose millions in business if people hear that it's breaking its confidentiality promises. But I think it would be constitutional for the government to try to increase contractual compliance either by providing an extra incentive for aggrieved parties to sue or by bringing a complaint itself. Though breach of contract has traditionally been seen as a purely private wrong, to be remedied through a private lawsuit, it's similar enough—especially when it's willful—to fraud or false advertising that there's nothing startling about a government agency such as the Federal Trade Commission prosecuting some such breaches itself.[38]

---

37. *Cf.* Kang, *supra* note 28, at 1267-68, 1280-81 (taking the same view). This might suggest that *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), is mistaken; the FCC regulations struck down by that case could be interpreted as just a default rule implementing customers' assumption that their telephone call data won't be used or disclosed without their permission.

Singleton, *infra* note 251, criticizes these sorts of default rules on policy grounds; I take no opinion on the policy question, but only argue that such rules are constitutionally permissible.

38. *But see* note 34 *supra* (discussing the possible *R.A.V. v. City of St. Paul* problem).

The great free speech advantage of the contract model is that it does *not* endorse any right to "stop people from speaking about me." Rather, it endorses a right to "stop people from violating their promises to me." One such promise may be a promise not to say things, and perhaps there may even be special defaults related to such promises or special remedies for breaches of such promises. But in any event, the government is simply enforcing obligations that the would-be speaker has himself assumed.[39] And such enforcement, in my view, poses little risk of setting a broad precedent for many further restrictions, precisely because it is founded only on the consent of the would-be speaker, and thus cannot justify the many other restraints—such as the Communications Decency Act, database protection legislation, and so on—to which the speaker has not consented.

B. *Limitations*

Contract law protection, though, is distinctly limited, in two ways.

First, it only lets people restrict speech by parties with whom they have a speech-restricting contract, express or implied.[40] If I make a deal with a newspaper reporter under which he promises not to identify me as a source, I can enforce the deal against the reporter and the reporter's employer, whom the reporter can bind as an agent. But if a reporter at another news outlet learns this information, then that outlet can publish it without fear of a breach of contract lawsuit. Likewise, there are no First Amendment problems with an employer suing an employee for breach of an express or implied nondisclosure agreement, but if the employee leaks the information to a newspaper, the employer can't sue that newspaper, at least under the *Cohen v. Cowles Media* theory.[41] The newspaper simply hasn't agreed to anything that would waive its First Amendment rights, which is the premise on which *Cohen v. Cowles Media* rests. The disclosure tort would similarly not be justifiable under a contract theory.

Second, *Cohen v. Cowles Media* cannot validate speech-restrictive terms that the government compels a party to include in a contract; the case at most validates government-specified defaults that apply unless the offeror makes clear that these terms aren't part of the offered deal. Thus, while the government may say "Cyberspace sales contracts shall carry an implied warranty that the seller promises not to reveal the buyer's personal information," it

---

39. *See* Cohen v. Cowles Media, 501 U.S. 663, 671 (1991).

40. As my colleague Jerry Kang pointed out to me, the contract theory might also apply when one merchant passes information about a customer to another merchant on the condition that the second merchant keep the information confidential, the second merchant breaches the condition, and then the customer sues on a third-party beneficiary theory.

41. Courts could hold the newspaper liable only by creating a new exception for downstream uses of unlawfully leaked information. *See* notes 95-96 *infra*.

may not add "and this implicit warranty may not be waived, even by a prominent statement that is explicitly agreed to by a customer clicking on an 'I understand, and agree to the contract in spite of this' button."

This flows directly from the rationale on which *Cohen v. Cowles Media* rests: "The parties themselves . . . determine the scope of their legal obligations, and any restrictions which may be placed on the publication of truthful information are self-imposed."[42] A merchant's express promise of confidentiality is "self-imposed"; so, one can say, is an implicit promise, when the merchant had the opportunity to say "by the way, I am not waiving my rights to speak about this transaction and am thus not promising confidentiality" but didn't do so. But when someone is legally barred from communicating, even if he explicitly told his contracting partner that he was making no such promise, then such an obligation is hardly "self-imposed" or determined by mutual agreement.

Thus, I certainly do not claim that a contractual approach to information privacy, even with a large dollop of implied contract, is a panacea for information privacy advocates. As Paul Schwartz and others have pointed out, there is much that information privacy advocates may want but that contract will not provide.[43] I claim only that contractual solutions are a constitutional alternative and may be the only constitutional alternative, not that they are always a particularly satisfactory alternative.

C. *Government Contracts*

Cohen v. Cowles Media does not decide to what extent the government, acting as contractor, may require people to sign speech-restrictive contracts as a condition of getting data from the government itself. This question raises thorny issues of unconstitutional conditions and often of the government's right to restrict access to government records that have historically been in the public domain (such as court records). Unfortunately, the Supreme Court case that some thought would help resolve this matter was decided on procedural grounds,[44] and the dicta in the many opinions in that case shed little light on exactly where the Court would have come down had it confronted the question on the merits.[45] I deal with this issue by setting it aside.

---

42. *Cohen v. Cowles Media*, 501 U.S. at 671.

43. *See* Schwartz, *supra* note *, at 1565-67.

44. Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999).

45. *Compare id.* at 490 (Scalia, J., joined by Thomas, J., concurring) (seeming to suggest that some such access restrictions might be unconstitutional) *and id.* at 493 (Stevens, J., joined by Kennedy, J., concurring) (concluding that the access restriction in that case was indeed unconstitutional) *with id.* at 491 (Ginsburg, J., joined by O'Connor, Souter, and Breyer, JJ., concurring) (seeming to take the opposite view).

D. *Contracts with Children*

Finally, this discussion of contracts presupposes that both parties are legally capable of entering into the contract and of accepting a disclaimer of any implied warranty of confidentiality. If a cyber-consumer is a child, then such an acceptance might not be valid. This is also a difficult issue, but one that is outside the scope of this Article.[46]

III. PROPERTY

A. *Intellectual Property Rules as Speech Restrictions*

Partly because of the limitations of the contract theory, many information privacy advocates argue that people should be assigned a property right in personal information about themselves.[47] Such a property approach would bind everyone, and not just those who are in contractual privity with the person being talked about. Database operators would have to stop communicating information about people unless people give permission, even though the database operators have never promised, expressly or implicitly, to keep silent. Likewise, people could stop newspapers from publishing stories about them, even if the information was gleaned through interviews with third parties or was taken (with no contractual constraints) from public records.[48]

Calling a speech restriction a "property right," though, doesn't make it any less a speech restriction, and it doesn't make it constitutionally permissible. Broad, pre-*New York Times v. Sullivan* libel laws can be characterized as protecting a property right in reputation; in fact, some states consider reputation a property interest.[49] The right to be free from interference with

---

46. *Cf.* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 *et seq.*; Matlick, note 245 *infra*; Singleton, *infra* note 251, text accompanying nn.76-79.

47. *See, e.g.*, Lawrence Lessig, *The Architecture of Privacy*, VAND. J. ENT. L. & PRAC., April 1999, at 56, 63 (suggesting that the law should give "individuals the [property] rights to control their data"); Carl Shapiro & Hal R. Varian, *US Government Information Policy*, <http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html>; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996); ALAN F. WESTIN, PRIVACY AND FREEDOM 324-25 (1967); Cohen, *supra* note 10, at 1420 (suggesting that "personally-identified data" may be treated as "the property or quasi-property of the individual to whom it refers").

48. *See* Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 439-40 (1978).

49. Reputation is generally not a property interest for purposes of the federal Due Process Clause, Paul v. Davis, 424 U.S. 693 (1976), but it can be a property right for other purposes. *E.g.*, Marrero v. City of Hialeah, 625 F.2d 499, 514 (5th Cir. 1980) (Florida law recognizes business reputation as a property interest); Nossen v. Hoy, 750 F. Supp. 740, 743 (E.D. Va. 1990) ("an individual holds a ... property interest in his or her reputation" for purposes of Washington and Virginia conversion law).

business relations, including interference by speech urging a boycott as in *NAACP v. Claiborne Hardware*,[50] is often seen as a property right.[51] A recent attempt at banning flag burning rested on the argument that the flag is the intellectual property of the United States, and that flag desecration thus violated property rights.[52] Restrictions on speech that uses cultural symbols in ways that the cultures find offensive might likewise be reframed as property rights in those symbols.[53] A ban on all unauthorized biographies, whether of former child prodigies,[54] movie stars, or politicians, can be seen as securing a property interest in the details of those people's lives. Similarly, an early right of publicity case took the view that people who aren't public figures have the exclusive right to block all photos and portraits of themselves, with no exceptions for news stories.[55]

Each of these "property rights," though, would remain a speech restriction.[56] A property right is, among other things, the right to exclude others;[57]

---

50. 458 U.S. 886 (1982).

51. "[T]he common law has long held that the reasonable expectancy of a prospective contract is a property right to be protected from wrongful interference in the same sense as an existing contract is protected." Leonard Duckworth, Inc. v. Michael L. Field & Co., 516 F.2d 952, 955 (5th Cir. 1975); *see also, e.g.*, City of Birmingham v. Business Realty Inv. Co., 722 So. 2d 747, 752 (Ala. 1998) (concluding that the "right to conduct a business relationship is an intangible property right" and is protected by the tort of "intentional interference with business relations").

52. H.R. 3883, 104th Cong., 2d Sess. (Rep. Torricelli); *see also* Texas v. Johnson, 491 U.S. 397, 429-30 (1989) (Rehnquist, C.J., dissenting) (suggesting that the government could ban flag desecration because it had a "limited [intellectual] property right" in the flag). *But see* United States v. Eichman, 496 U.S. 310 (1990) (holding that flag burning is protected speech); Texas v. Johnson, 491 U.S. 397 (1989) (same).

53. *Cf.* Hornell Brewing Co. v. Rosebud Sioux Tribal Court, 133 F.3d 1087 (8th Cir. 1998) (involving the descendants of the Sioux leader Crazy Horse, then 115 years dead, trying to use right of publicity law to stop the marketing of Crazy Horse Malt Liquor; the malt liquor company won on procedural grounds).

54. *Cf.* Sidis v. F.R. Pub. Co., 113 F.2d 806 (2d Cir. 1940) (holding that a publisher could not be held liable for publishing an accurate biographical article about a former child prodigy); *but cf.* Bloustein, *infra* note 179, at 66-70 (arguing that the former child prodigy should have won).

55. Corliss v. E.W. Walker Co., 64 F. 280, 282 (C.C.D. Mass. 1894) ("[A] private individual has a right to be protected in the representation of his portrait in any form; . . . this is a property as well as a personal right . . . . A private individual should be protected against the publication of any portraiture of himself . . . .").

56. *See* International Olympic Comm. v. San Francisco Arts & Athletics, 789 F.2d 1319, 1321 (9th Cir. 1986) (Kozinski, J., dissenting from denial of rehearing en banc) ("To say that the word Olympic is property begs the question. What appellants challenge is the power of Congress to privatize the word Olympic, rendering it unutterable by anyone else in connection with any product or public event, whether for profit or, as in this case, to promote a cause."); Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1537 (1993) (expressing concern that in some arguments "the incantation 'property' seems sufficient to render free speech issues invisible"); Dianne Lenheer Zimmerman, *Information as Speech, Information as Goods*, 33 WM. & MARY L. REV. 665 (1992) (expressing concern that "[w]ithout better principles for confining the sphere of property rules, the likely outcome is that more and more chunks of communicative activity will fall on the property side of the line").

an intellectual property right in information is the right to exclude others from communicating the information—a right to stop others from speaking. Like libel law, intellectual property law is enforced almost entirely through private litigation, but like libel law, it's still a government-imposed restriction on speech.[58] Some such restrictions may be permissible because there's some substantive reason why it's proper for the government to restrict such speech, but not *because* they are intellectual property rights.

The question isn't (as some suggest) "who should own the property right to personal information?"[59] Rather, it's whether personal information should be treated as property at all—whether some "owner" should be able to block others from communicating this information, or whether everyone should be free to speak about it.

B. *Existing Restrictions as Supposed Precedents*

The Court has, of course, upheld some intellectual property rights against First Amendment challenge, acknowledging that they are speech restrictions but holding that those restrictions were constitutional. In all these precedents, though, the Court has stressed a key point: The restrictions did not give the intellectual property owners the power to suppress facts. And this power to suppress facts is exactly the power that information privacy speech restrictions would grant.[60]

---

57. *See, e.g.*, College Savings Bank v. Florida Prepaid Postsecondary Ed. Expense Bd., 119 S. Ct. 2219, 2224 (1999) ("The hallmark of a protected property interest is the right to exclude others."); Kaiser Aetna v. United States, 444 U.S. 164, 179-80 (1979) ("the 'right to exclude' [is] universally held to be a fundamental element of the property right").

58. *See, e.g.*, New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964); *see also* Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (intentional infliction of emotional distress law applied to speech is a speech restriction even though it is enforced through private lawsuits); NAACP v. Claiborne Hardware, 458 U.S. 886 (1982) (holding likewise as to the law of intentional interference with business relations).

59. *See, e.g.*, Murphy, *supra* note 47, at 2393 ("[P]ersonal information is, in fact, property. Thus, the net effect—in economic terms—of the failure of the disclosure tort has been to assign the property right to personal information to the party who uncovers the information, rather than to the party whom the information concerns."). A recent article seems to take the same view, concluding that recent cases striking down information privacy speech restrictions "implicit[ly]" assumed that personally identified data is information "owned, presumptively, by those who collect it." Cohen, *supra* note 10, at 1413. I disagree: In my view, those cases implicitly rested on the notion that facts are not owned by anyone, and that everyone is thus free to communicate them.

60. *See generally* Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. VS 8, *available at* <http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8/> (concluding that traditional intellectual property law provides little support for informational privacy speech restrictions); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1136-46 (2000) (same); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1294-95 (2000) (concluding that a property rights approach to information privacy speech restrictions is unsound because it would improperly create an intellectual property right in facts).

1. *Copyright law.*

Harper & Row v. Nation Enterprises, which held that copyright law is constitutional,[61] is the best example of this. Under copyright law, I may not publish a book that includes more than a modicum of creative expression from your book, even though my book is neither obscene nor libelous nor commercial advertising; such a restriction, *Harper & Row* held, is indeed a speech restriction, but a permissible one.

But the main reason *Harper & Row* gave for this conclusion is that copyright law does not give anyone a right to restrict others from communicating facts or ideas. "[C]opyright's idea/expression dichotomy strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting *free communication of facts* while still protecting an author's expression."[62] "No author may copyright his ideas or *the facts he narrates."*[63] Copiers "possess[] an unfettered right to use *any factual information* revealed in [the original]," though they may not copy creative expression.[64] There ought not be "abuse of the copyright owner's monopoly as an instrument to suppress *facts*."[65] "In view of the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and *uncopyrightable facts* and ideas," copyright law is constitutional.[66] Under the copyright exception to free speech protection, then, speech that borrows creative expression is restrictable, but speech that borrows only facts remains free.

This limitation on the copyright exception is both theoretically and practically significant. Theoretically, this limitation is what leaves speakers ample alternative channels for communicating their message—speakers still possess "an unfettered right to use any factual information" that they please. Practically, people do indeed take advantage of this limitation. If a historian spent years of effort uncovering some remarkable, hitherto unknown facts, you may freely use those facts, as historians indeed do (though ethical rather than legal concerns may dictate that the users give credit to the original discoverer). Exactly where to draw the line between idea and expression is sometimes uncertain, but there are fewer uncertainties about the line between fact and expression; people who don't care about using the original author's rhetorical flourishes can definitely communicate facts that they've learned from others' work.

---

61. 471 U.S. 539 (1985).

62. *Id.* at 556 (emphasis added and internal quotation marks omitted).

63. *Id.* (emphasis added).

64. *Id.* at 557-58 (emphasis added) (quoting Iowa State Univ. Research Found., Inc. v. American Broad. Cos., 621 F.2d 57, 61 (2d Cir. 1980)).

65. *Id.* at 559 (emphasis added).

66. *Id.* at 560 (emphasis added). *See also* Singleton, *infra* note 251, at text accompanying n.68 (making a similar observation about copyright law).

2. *Trademark law.*

Likewise with trademark law. Though trademark law restricts certain uses of trademarks in advertising a product or on the cover of the product, it does not prohibit speech that communicates facts or opinions about the product, even if the speech uses the product's name. You are free to write a book about the Coca-Cola Company—a book that will be commercially sold, but that is itself not commercial speech because it's not commercial advertising—or a book describing the nutritional qualities of various soft drinks, or even a novel in which the main character constantly drinks Diet Cokes.[67] Likewise, if you're distributing or selling product reviews or a table mapping product names to cost and quality, you don't need permission from the trademark owner. Even in ads, factually accurate statements about the relationship of your products to others' products are permitted, either because they are in context not misleading or because they fall under the rubric of "nominative fair use."[68] The new federal trademark dilution statute, which has not yet been considered by the Court, also follows this principle; it is limited to commercial advertising, and even there provides a fair use defense.[69]

Even the *Gay Olympics* case,[70] which involved an unusually broad quasi-trademark law that gave the U.S. Olympic Committee the exclusive right to use the word "Olympic" for advertising and promotional purposes, stressed this point: "By prohibiting the use of one word for particular purposes, neither Congress nor the USOC has prohibited the [plaintiff] from conveying its message."[71] The case did not involve any congressional attempt to let the USOC stop people from discussing the Olympics, conveying facts about the Olympics, writing fiction about the Olympics, and so on.[72] Even given this

67. *See* White v. Samsung Elecs. Am., Inc., 989 F.2d 1512, 1512 & n.6 (9th Cir. 1992) (Kozinski, J., dissenting from denial of rehearing en banc).

68. *See, e.g.*, New Kids on the Block v. News Am. Publ., Inc., 971 F.2d 302, 308 (9th Cir. 1992).

69. *See* Federal Trademark Dilution Act of 1995, 15 U.S.C. §§ 1125(c)(1), (c)(4). I'm not a great fan of the dilution statute, for reasons expressed by Lemley, *see* note 114 *infra*, and Pollack, *see* note 117 *infra*; and some recent decisions under it, especially *Jews for Jesus v. Brodsky*, 993 F. Supp. 282 (D.N.J. 1998) (granting a preliminary injunction against a fundamentally noncommercial use of an internet domain name substantially similar to the name of plaintiff's organization), strike me as mistaken. Still, if properly applied, the statute at least does not restrict the free communication of facts.

70. San Francisco Arts & Athletics, Inc. v. United States Olympic Comm., 483 U.S. 522 (1987).

71. *Id.* at 536.

72. *See, e.g.*, Stop the Olympic Prison v. United States Olympic Comm., 489 F. Supp. 1112, 1118-21 (S.D.N.Y. 1980) (holding that the use of an Olympic logo and an Olympic torch on a poster opposing the planned conversion of an Olympic Village into a prison did not violate the statute); *San Francisco Arts & Athletics*, 483 U.S. at 536 & n.14 (stating that the statute might not "restrict[] purely expressive uses of the word 'Olympic,'" citing *Stop the Olympic Prison*); *id.* at

limitation, the law considered in the *Gay Olympics* case has been criticized as going too far,[73] and I generally agree with these criticisms. But even if the law improperly gave the USOC too much power, it didn't give it the power to stop the communication of facts.

3. *Right of publicity law.*

The same is true of *Zacchini v. Scripps-Howard Broadcasting Co.*, in which the Supreme Court endorsed a narrow subset of the right of publicity: a right to block others from retransmitting one's entire performance.[74] *Zacchini* concluded that a TV station's rebroadcast of Hugo Zacchini's entire human cannonball act was restrictable for the same reasons that copyright infringement was restrictable;[75] and, as it would eventually do as to copyright, the Court stressed that the law did not restrict the communication of facts. The case would have been "very different," the Court said, if "respondent had merely reported that petitioner was performing at the fair and described or commented on his act, with or without showing his picture on television";[76] liability was permissible because it was based not just on for-profit "reporting of events" but on "broadcast[ing] or publish[ing] an entire act for which the performer ordinarily gets paid."[77]

The Supreme Court has never confronted the broader right to restrict speech that uses one's name or likeness; *Zacchini* explicitly stressed that it wasn't deciding anything about this right,[78] and though some courts and commentators have omitted this critical limitation and have cited *Zacchini* as

---

539-40 (describing the statute as applying to uses of the word "to induce the sales of goods or services" and to other "promotional uses").

73. *See, e.g.*, International Olympic Comm. v. San Francisco Arts & Athletics, 789 F.2d 1319, 1320 (9th Cir. 1986) (Kozinski, J., dissenting from denial of rehearing en banc); Robert N. Kravitz, *Trademarks, Speech, and the Gay Olympics Case*, 69 B.U. L. REV. 131 (1989).

74. 433 U.S. 562 (1977).

75. *Id.* at 573, 576-77.

76. *Id.* at 569.

77. *Id.* at 574.

78. "It should be noted . . . that the case before us is more limited than the broad category of lawsuits that may arise under the heading of 'appropriation.' Petitioner does not merely assert that some general use, such as advertising, was made of his name or likeness; he relies on the much narrower claim that respondent televised an entire act that he ordinarily gets paid to perform." *Id.* at 573 n.10. "[T]he broadcast of petitioner's entire performance, unlike the unauthorized use of another's name for purposes of trade or the incidental use of a name or picture by the press, goes to the heart of petitioner's ability to earn a living as an entertainer. Thus, in this case, Ohio has recognized what may be the strongest case for a 'right of publicity' involving, not the appropriation of an entertainer's reputation to enhance the attractiveness of a commercial product, but the appropriation of the very activity by which the entertainer acquired his reputation in the first place." *Id.* at 576. The Court repeated several times that the case involved the broadcast of "a performer's entire act." *Id.* at 570, 574, and twice at 575.

generally "hold[ing] that the right of publicity is constitutional,"[79] such a characterization is mistaken. But even to the extent that lower courts have recognized such a right, they too have adopted limiting principles that keep the right from restraining the communication of facts.

To begin with, though the right of publicity is sometimes described as a right to stop others from using one's name, likeness, and other attributes of identity "in commerce" or "for trade purposes,"[80] courts and legislatures have long recognized that use of name or likeness "in news reporting, commentary, entertainment, or in works of fiction or nonfiction"[81] must be excluded. These uses are sold in commerce and in trade, but they are nonetheless protected from right of publicity claims, in large part because of free speech concerns.[82] The right is not allowed to stop the communication of facts about a celebrity, even if it is allowed to block advertising or merchandising that merely tries to associate the advertiser or the consumer with a celebrity.

Moreover, even the use of name or likeness in an advertisement that is incidental to the permitted uses—for instance, a billboard advertising an unauthorized biography, which will necessarily use the subject's name and probably likeness—is likewise excluded from the right of publicity, though it's clearly "in commerce" and "for trade purposes."[83] This again relates directly to the need to prevent the suppression of facts. Letting Elizabeth Taylor block the unauthorized use of her name in ads for clothing would

79. *See, e.g.*, Comedy III Prods., Inc. v. Gary Saderup, Inc., 80 Cal. Rptr. 2d 464, 471 (Ct. App. 1998) (stating, in a context quite unrelated to the one in *Zacchini*, that *Zacchini* "considered, and rejected, a First Amendment defense to liability for infringement of the right of publicity"); Lorin Brennan, *The Public Policy of Information Licensing*, 36 HOUS. L. REV. 61, 99-100 (1999) (characterizing *Zacchini* as upholding the protection of the "right of publicity," defined by the author as the right to stop "misappropriation of name or likeness").

80. *See, e.g.*, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 (Tentative Draft No.4, 1993) ("One who appropriates the commercial value of a person's identity by using without consent the person's name, likeness, or other indicia of identity for purposes of trade is subject to liability ....").

81. *Id.* § 47.

82. *See, e.g.*, Hicks v. Casablanca Records, 464 F. Supp. 426 (S.D.N.Y. 1978) (fictionalized account of episode in life of Agatha Christie); Eastwood v. Superior Court, 198 Cal. Rptr. 342, 350 (Ct. App. 1983) (newspaper article about Clint Eastwood); Frosch v. Grosset & Dunlap, Inc., 427 N.Y.S.2d 828 (App. Div. 1980) (book about Marilyn Monroe); Guglielmi v. Spelling-Goldberg Productions, 603 P.2d 454, 455 (Cal. 1979) (Bird, C.J., concurring) (fictionalized account of life of Rudolph Valentino).

83. *See, e.g.*, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 47 cmt. a (Tentative Draft No.4, 1993) (stating the same rule as a matter of substantive right of publicity law); Cher v. Forum Int'l, Ltd., 692 F.2d 634, 639 (9th Cir. 1982) ("Forum would have been entitled to use Cher's picture and to refer to her truthfully in subscription advertising for the purpose of indicating the content of the publication, ... because such usage is protected by the First Amendment."); Page v. Something Weird Video, 960 F. Supp. 1438, 1443 (C.D. Cal. 1996) (stating that "[p]romotional speech may be noncommercial if it advertises an activity itself protected by the First Amendment," and upholding against a right of publicity claim the right to advertise videos by using the likeness of one of the stars).

rarely substantially interfere with the manufacturer's ability to convey the facts about the clothing. Letting her block the use of her name in ads for an unauthorized biography, however, would mean that the biographer couldn't communicate to potential buyers the critical fact that the book is about Taylor.

The right of publicity may have gotten too big,[84] but even it basically respects the principle that there ought to be no "abuse of the [intellectual property] owner's monopoly as an instrument to suppress facts";[85] supporters of property rights in facts thus can't get much analogical support out of it. For whatever it's worth, the few cases that have considered right of publicity claims based on the sale of databases containing personal information have rejected such claims.[86]

4. *Misappropriation and trade secret law.*

The above discussion has covered all the intellectual property speech restrictions that the Court has upheld against a First Amendment challenge. There are two other quasi-intellectual-property rules that may purport to confer limited property rights in facts, but the Court has never considered whether these speech restrictions are constitutional.

The first such rule is the right to be free from "unfair" misappropriation of hot news (and possibly of other information). This right was recognized by the Court in 1918 in *International News Service v. Associated Press* as a matter of pre-*Erie* federal common law,[87] but has been mostly rejected since then, most prominently by the Restatement (Third) of Unfair Competition.[88]

Perhaps because this tort has largely (though not entirely[89]) withered, the Court has never decided whether it passes muster under the First Amendment. Certainly the 1918 decision recognizing the tort didn't confront a First Amendment defense, and in any event First Amendment protections have been dramatically strengthened since then. I believe that if the Court does

84. *See, e.g.*, Cardtoons, L.C. v. Major League Baseball Players Ass'n, 95 F.3d 959, 970 (10th Cir. 1996); White v. Samsung Elecs. Am., Inc., 989 F.2d 1512, 1520 (9th Cir. 1992) (Kozinski, J., dissenting from denial of rehearing en banc); Madow, *infra* note 111; Zimmerman, *infra* note 220.

85. Harper & Row, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985).

86. *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351, 1356 (Ill. App. 1995); Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio App. 1975).

87. 248 U.S. 215 (1918).

88. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 cmts. b & c (Tentative Draft No. 4, 1993) (criticizing *INS v. AP* and reporting that most courts have not followed it). As with the proposed database protection law, *see infra* note 112, the hot news tort secures a right that's in some respects narrower and in some respects broader than traditional intellectual property rights; but for the purposes of this discussion, what is important is that this right is a right to exclude others from certain uses of the plaintiff's information, and is thus a quasi-property right.

89. *See* NBA v. Motorola, Inc., 105 F.3d 841, 847-48, 853 (2d Cir. 1997) (inferring that state courts would still recognize the tort, but fortunately limiting it to only a narrow range of hot news).

confront this question, it should conclude that such a right to stop others from communicating hot news is indeed an unconstitutional content-based restriction on fully protected speech.[90]

The second such quasi-property right is secured by trade secret law. Trade secret protection generally flows from a contract, express or implied, between the trade secret owner and the defendant who is threatening to use or expose the secret;[91] in such a case, *Cohen v. Cowles Media* strongly suggests that the defendant can be held to the bargain.[92] Occasionally, trade secret claims may be based on illegal acquisition (for instance, through a trespass) by the defendant; certainly such acquisition can be punished without First Amendment difficulties.[93]

The serious First Amendment problems arise when a trade secret owner seeks to restrict the speech of those who are not in contractual privity with it,[94] for instance when a company whose employees leaked secret information to a newspaper wants to enjoin the newspaper from publishing the information. The newspaper has never promised anyone not to speak about this, so *Cohen v. Cowles Media* doesn't apply; the speech restriction can be justified only on the theory that the leaker's initial violation of his confiden-

---

90. Recent Supreme Court cites to *INS v. AP* are unilluminating. *San Francisco Arts & Athletics v. United States Olympic Comm.*, 483 U.S. 522 (1987), did cite *INS* with some seeming approval, *id.* at 532, but it certainly did not explicitly pass on the constitutionality of a hot news misappropriation tort. Nor was it asked to do so; the decision primarily focused on the commercial speech doctrine, which is inapplicable to hot news misappropriation cases. *Harper & Row* cited *INS* only for the proposition that *copyright law* does not create a property rights in fact, and in the same paragraph said that "copyright's idea/expression dichotomy strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression." 471 U.S. 539, 556 (1985) (internal quotation marks omitted). Finally, Chief Justice Rehnquist's dissent in *Texas v. Johnson*, 491 U.S. 397 (1989), indirectly cited *INS v. AP* as support for the notion that flag burning laws may be justified on intellectual property grounds—in my view, evidence that the recognition of broad, First-Amendment-proof intellectual property rights does indeed risk further broadening of speech restrictions.

91. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (Tentative Draft No.4, 1993) (defining the most common type of trade secret as flowing from "an express promise of confidentiality" or from circumstances in which the trade secret owner reasonably inferred such a promise and the party to be bound should have realized this).

92. *See* text accompanying notes 29-39; *cf.* Cherne Indus., Inc. v. Grounds & Assocs., Inc., 278 N.W.2d 81, 94 (Minn. 1979) (pre-*Cohen v. Cowles Media* case holding that "a former employee's use of confidential information or trade secrets of his employer in violation of a contractual or fiduciary duty is not protected by the First Amendment"—the court was referring here to fiduciary duties flowing from the employer-employee contract).

93. *See generally* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (Tentative Draft No.4, 1993); Lemley & Volokh, *infra* note 119, at 230.

94. *See, e.g.*, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 ("One is subject to liability for the appropriation of another's trade secret if . . . (b) the actor . . . discloses the other's trade secret . . . and, at the time of the . . . disclosure, (3) the actor knows or should know that the information is a trade secret that the actor acquired from or through a person who acquired it by means that are improper under the rule stated in § 43 or whose disclosure of the trade secret . . . constituted a breach of a duty of confidence owed to . . . the other under the rule stated in §§ 41 and 42").

tiality promise bars otherwise innocent third parties from reporting on the leaked information. The same issue arises in other confidential information contexts, for instance when a newspaper publishes information illegally leaked by a government employee, or illegally taped by someone who then passed along the tape recording.

The Supreme Court has never decided whether such speech restrictions are constitutional, and lower courts are divided on the subject. I think those courts that come out against such speech restrictions have it right: Speech by people who have never promised to remain quiet about something may not be suppressed simply because someone else wrongfully revealed the information to them. Newspapers must be able to publish leaked information (at least absent some overwhelming national security concerns), even if the leaker breached a contract or even broke the law; a contrary rule would dramatically undermine newspapers' ability to report.[95] Intercepting confidential communications is properly outlawed, but a newspaper need not stay silent about such communications if they come into the newspaper's hands.[96]

---

95. *Cf.* Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 837 (1978) (holding that the First Amendment does not "permit[] the criminal punishment of third persons who are strangers to the inquiry, including the news media, for divulging or publishing truthful information regarding confidential proceedings of the Judicial Inquiry and Review Commission," even though the media in that case apparently got the information as a result of someone's breach of his obligation of confidentiality); CBS Inc. v. Davis, 510 U.S. 1315 (1994) (Blackmun, J., in chambers) (staying on First Amendment grounds an injunction that barred a television station from broadcasting material that allegedly revealed trade secrets); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999) (holding that enjoining a Web site from communicating leaked material would violate the First Amendment); Oregon *ex rel.* Sports Management News, Inc. v. Nachtigal, 921 P.2d 1304 (Or. 1996) (holding that enjoining a newsletter from publishing a trade secret would violate the Oregon Constitution's free speech protections); Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260, 262-63 (E.D. Va. 1995) (holding that enjoining a person from posting confidential to the Web would violate the First Amendment); and Pearson v. Dodd, 410 F.2d 701 (D.C. Cir. 1969) (rejecting, on tort law grounds, liability for a columnist's publication of documents that he knew were illegally leaked); *see also* Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219 (6th Cir. 1996) (holding that enjoining a magazine from publishing material leaked to it in violation of a discovery protective order violated the First Amendment). *Compare generally* Robert M. O'Neil, *Tainted Sources: First Amendment Rights and Journalistic Wrongs*, 4 WM. & MARY BILL RTS. J. 1005, 1019-21 (1996) (exploring the limits of First Amendment protections for publication of improperly released information subject to court protective orders) *with* Giles T. Cohen, Comment, *Protective Orders, Property Interests and Prior Restraints*, 144 U. PA. L. REV. 2463 (1996) (advocating broader court powers to suppress publication of such materials). *But see* Garth v. Staktek Corp., 876 S.W.2d 545 (Tex. App. 1994) (holding constitutional, without an extensive discussion, an injunction against revelation of trade secrets by a downstream speaker). All these cases, though, arose from attacks on injunctions under the prior restraint doctrine; I've found no decisions that squarely decide whether damages liability based on the downstream revelation of trade secrets leaked to third parties would violate the First Amendment.

96. *Compare* Boehner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999) (holding that the federal bar on the communication of intercepted communication may constitutionally be applied to downstream speakers who did not themselves illegally intercept anything) *with* Bartnicki v. Vopper, 200 F.3d 109 (3rd Cir. 1999) (holding that such a speech restriction is unconstitutional) *and* Peavy v. Harman, 37 F. Supp. 2d 495, 516-18 (N.D. Tex. 1999) (same as *Bartnicki*), *appeal docketed*; *see also Boehner*, 191 F.3d at 480 (Sentelle, J., dissenting); *Bartnicki*, 200 F.3d at 129 (Pollak, J., dis-

People shouldn't be legally forbidden from telling their friends the truth about someone's medical condition (for instance, that the friend's prospective lover is suffering from a contagious disease) even if the information originally came from a source who had no right to reveal it (such as the prospective lover's doctor).

Thus, there are no existing First Amendment exceptions that justify restrictions on communication of hot news and restrictions on the publication of illegally leaked facts. One could, of course, argue that the Court should create such new exceptions, but one can't argue that these exceptions already provide support for information privacy speech restrictions. Rather, as I argue below in Part III.D, it is Supreme Court recognition of a property-rights-based First Amendment exception for information privacy speech restrictions that would substantially strengthen the calls for a hot news exception and an illegally leaked facts exception.

5. *Summary.*

There are other limitations on many of these intellectual property rights that make any analogies to information privacy speech restrictions quite doubtful: For instance, copyright law and the *Zacchini* right are in large measure justified as necessary incentives for authors to create new works; likewise, most of trademark law and most of right of publicity law apply only to commercial advertising. But the core principle at the heart of all these restrictions is that they create a fairly narrow right that may affect the form of people's speech but ought not prevent people from communicating facts. Any putative right in one's personal information can thus be adopted by analogy only if one is willing to relax this limitation, a limitation that is critical to protecting free speech.[97]

C. *Functional Arguments for Upholding Information Privacy Speech Restrictions Under a Property Theory*

1. *Avoiding "free-riding" and unjust enrichment.*

Some argue for property rights in personal information on functional grounds: Those who communicate personal information about others are

---

senting). *But see* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 987, 1018-29 (2000) (forcefully arguing that restricting such third-party publication of secrets leaked or intercepted by others should indeed be constitutional).

97. *Cf.* Litman, *supra* note 60, at 1294 ("When we recognize property rights in facts, we endorse the idea that facts may be privately owned and that the owner of a fact is entitled to put restrictions on the uses to which that fact may be put. That notion . . . is inconsistent with much of our current first amendment jurisprudence.").

engaging in a sort of free riding, enriching themselves without compensating the people whose existence makes their enrichment possible; and property rights, the argument goes, are the way to avoid this free riding. As one article argued, in 1988 three leading credit bureaus made almost $1 billion put together from selling credit information, but "[h]ow much did these credit bureaus pay consumers for the information about them that they sold? Zero."[98]

This, though, cannot be the justification for restricting speech, unless we are willing to dramatically redefine free speech law. Newspapers and radio and TV news programs, after all, make billions from stories that are made possible only by the existence of their subjects. The essence of news is precisely the reporting of things done or discovered by others; the essence of the news business is profiting from reporting on things done or discovered by others. But news organizations generally don't pay a penny to the subjects of their stories—in fact, it is seen as unethical for news organs, though not entertainment organs, to pay subjects.[99] Likewise, unauthorized biographers and historians make money from publishing information about others, information that only exists because those people exist. Comedians who tell jokes about people make a living from those they mock.[100]

In a sense, all these speakers are free-riding: They are taking advantage of something that relates to someone else and that exists only because of that other person's existence, and they aren't paying that person for it (though they are usually investing a good deal of time, money, and effort in the project—this free-riding is certainly not mere literal copying). But our legal

98. Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1793 (1995).

99. *See, e.g.*, Rick Bentley, *Outreach Takes Station off the Sidelines*, FRESNO BEE, Oct. 7, 1999, at E3 ("Local television news teams have a prime directive: No payment for interviews. Checkbook journalism can destroy a news organization's credibility in an instant.").

100. In some of these examples, some (though not all) subjects of the speech do profit from the speech, albeit indirectly. The subject of a story may be pleased by his newfound fame; the manufacturer of a product that's covered favorably in the newspaper may make money as a result of the coverage. But of course other subjects of news stories are hurt, either financially or emotionally, by those stories; in such cases, the news organ may be making a profit at the same time that the subjects of the stories, without whom the stories would never have existed, are suffering a loss. Free speech law's response to these subjects is "tough luck," at least unless the stories say something false.

And in this respect, distribution of personal information databases is no different from the publishing of news. Many, perhaps most, of the subjects of these databases derive indirect benefits just like the subjects of news stories do. If I have a good credit history, I am benefited by the credit history databases—if the databases didn't exist and would-be creditors had no way of knowing my record, I'd have to pay a higher interest rate. Likewise, while many people are annoyed by having their personal information available to marketers, some people apparently find the targeted marketing useful, or else they wouldn't buy as a result of this marketing and the marketing would become unprofitable and stop. Thus, some (but not all) people indirectly benefit as a result of information about them being stored in databases—just as some (but not all) people indirectly benefit as a result of news stories about them or their businesses.

system correctly allows a great deal of free-riding. It has never been a principle of tort law that all free-riding is illegal, or that all such enrichment is unjust. In the words of the Restatement (Third) of Unfair Competition,

> [T]he principle of unjust enrichment does not demand restitution of every gain derived from the efforts of others. A small shop, for example, may freely benefit from the customers attracted by a nearby department store, a local manufacturer may benefit from increased demand attributable to the promotional efforts of a national manufacturer of similar goods, and a newspaper may benefit from reporting on local athletic teams. Similarly, the law has long recognized the right of a competitor to copy the successful products and methods of others absent an infringement of patent, copyright, or trademark rights.[101]

And it has certainly not been a principle of free speech law that speech may be restricted simply to assure the subject of the speech a piece of the profits.

What intellectual property law has generally tried to prevent is not free-riding as such, but free-riding of a particular kind: the use not just of something that relates to another, but the use of the product of another's substantial labor, and even that only in limited cases.[102] Such a use runs the risk of dramatically diminishing the incentive to engage in such labor, which is what makes the defendant's enrichment socially harmful rather than merely unjust in some abstract moral sense. This concern is at the heart of copyright law,[103] of the right to prevent the unauthorized transmission of an entire act,[104] and to a large extent of trade secret law. But this concern does not apply to personal information about people, where the incentive arguments don't really apply.

Again, I stress that my critique here only relates to the intellectual property justification for information privacy speech restrictions; perhaps there are some other justifications that can support such speech restraints. But the fact that information distributors are profiting while the subjects of the information does not itself provide such support.

2. *Internalizing costs and maximizing aggregate utility.*

Another functional argument often made on behalf of a property rights theory of information privacy speech restrictions is that the property rights model is the best way to require speakers to "internalize th[e] cost" of their

---

101. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 cmt. b (Tentative Draft No. 4, 1993).

102. *See* Dreyfuss, *supra* note 60 ("American law recognizes a privilege to copy. . . . For intellectual property, the traditional rationale for [departing from this baseline] is incentive-based. . . . Those who merely generate information as a byproduct of activities for which no special incentives are necessary are not, therefore, the traditional beneficiaries of intellectual property legislation.").

103. *See* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349 (1991).

104. Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 576 (1977). *See also* text accompanying notes 87 to 96 *supra* (discussing and criticizing the hot news misappropriation tort).

speech "by paying those whose data is used."[105] Such internalizing, the theory goes, would maximize aggregate social utility: By "recogniz[ing the] diversity" of people's desires for information privacy, the property rule could make sure that information about each person is communicated only if the benefit to the speaker exceeds the felt cost to the subject.[106]

The principle of free speech law, though, is that speakers do *not* have to internalize all the felt costs that flow from the communicative impact of their speech. The NAACP didn't have to internalize the tangible economic (not just emotional) cost that its boycott imposed on the Claiborne County merchants.[107] Movie producers don't have to internalize the tangible cost that their movies impose on victims of viewers who commit copycat crimes.[108] Cohen, Johnson, and Hustler didn't have to internalize the emotional distress cost that their speech inflicted on passersby or on its subject.[109]

Again, if there's an independent reason why this speech should be treated differently from other speech, for instance because it falls within some new free speech exception, then the law may require that its costs be internalized. But the desire to maximize aggregate social utility doesn't itself justify a new exception; on the contrary, it's only the new exception that would legitimize speech restraints aimed at maximizing aggregate social utility.

D. *The Potential Consequences*

I have explained why I think that merely calling information privacy speech restrictions "property rights" doesn't advance the First Amendment inquiry, why such speech restrictions aren't justifiable under any existing intellectual property exceptions, and why such monopolies in facts, not just

---

105. Lessig, *supra* note 47, at 63.

106. *See, e.g., id.*; Bloustein, *supra* note 48, at 439-40 (endorsing the property rights theory on the grounds that it fosters "a process of voluntary exchange, [that,] like the free market generally, would assure that 'human satisfaction as measured by aggregate consumer willingness to pay . . . is maximized'"); Murphy, *supra* note 47, at 2395-96.

107. NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982).

108. *E.g.*, Olivia N. v. NBC, Inc., 178 Cal. Rptr. 888 (Ct. App. 1981) (barring recovery where child was sexually abused by minors who allegedly copied a similar crime shown on television); Bill v. Superior Court, 187 Cal. Rptr. 625 (Ct. App. 1982) (barring recovery where girl was shot outside theater by a moviegoer who was allegedly copying a violent scene from the movie); *see also* DeFilippo v. NBC, Inc., 446 A.2d 1036 (R.I. 1982) (barring recovery for parents whose child hanged himself after watching a mock hanging); Walt Disney Prod., Inc. v. Shannon, 276 S.E.2d 580 (Ga. 1981) (barring recovery where child hurt himself while trying to duplicate a sound effect technique demonstrated on a television program).

109. Cohen v. California, 403 U.S. 15 (1971) (public profanity constitutionally protected); Texas v. Johnson, 491 U.S. 397 (1989) (public flag burning constitutionally protected); Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (vicious personal attack constitutionally protected).

expression, are theoretically troubling.[110] Of course, despite all this, the Court is always free to carve out a new First Amendment exception or broaden an existing one; my goal now is to explain why I think this would be a bad idea.

Speech that reveals private information is not the only speech that some want to restrict under the property rights model. As many leading commentators have recently argued, we are now in the midst of a broad movement that uses intellectual property rhetoric to broaden people's rights to restrict others' speech.[111] The proposed database protection legislation would give database owners a form of property right in collections of information.[112] Some recent cases have revived the misappropriation tort, recognizing a property right in news.[113] Many recent cases have broadened trademark owners' rights to restrict parodies and other transformative uses (though

---

110. *Cf.* Zimmerman, *supra* note 56, at 733 (arguing that the idea/expression line—which in copyright law also distinguishes facts from expression—"has great merit as a line of demarcation on First Amendment and not merely on intellectual property grounds," and that any property rights in information should respect this line).

111. *See, e.g.*, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 354 (1999) ("We are in the midst of an enclosure movement in our informational environment."); Mark A. Lemley, *Romantic Authorship and the Rhetoric of Property*, 75 TEX. L. REV. 873, 898 (1997) ("[T]here is currently a strong tendency to 'propertize' everything in the realm of information. Intellectual property law is expanding on an almost daily basis as new rights are created or existing rights are applied to give intellectual property owners rights that they never would have had in an earlier time."); Jessica Litman, *Reforming Information Law in Copyright's Image*, 22 DAYTON L. REV. 587, 593 (1997) (arguing that there is a "serious effort . . . afoot to refashion our information policy to give primacy to intellectual property laws"); Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 125, 142 (1993) ("In recent decades . . . the law has moved more and more of our culture's basic semiotic and symbolic resources out of the public domain and into private hands."); David Lange, *Recognizing the Public Domain*, 44 LAW & CONTEMP. PROBS. 147, 171 (1981); Zimmerman, *infra* note 220, at 51:

> Indeed, we live in the era when intellectual property has became king of the hill. Lawmakers and creative individuals alike increasingly treat as received truth the contestable intuition that producers of intellectual products should have a "right" to any income stream their labor can generate. They label as immoral and self-serving counterarguments that, except in narrowly tailored circumstances, intangible intellectual contributions with value to the public should be freely appropriable. This pro-property mind set has been further encouraged by the gradual recognition that income from intellectual property makes up a very significant part of the United States' balance of payments in the international trade arena. In short, a claimant who says that someone is "stealing" his intellectual labor is making an assertion of greater attractiveness to the modern legal ear than someone who makes the counter-argument that all these property claims are diminishing the ability of others to express themselves.

112. *See* Benkler, *supra* note 111, at 358, 440, 445-46. The law would secure a right that's in some respects narrower and in some respects broader than traditional intellectual property rights, but for the purposes of this discussion, what is important is that this right would be a right to exclude others from certain uses of the plaintiff's information, and would thus be a form of property right.

113. *See, e.g.*, NBA v. Motorola, Inc., 105 F.3d 841, 853 (2nd Cir. 1997) (fortunately limiting the tort to only a narrow range of hot news).

fortunately some courts seem to be resisting this trend).[114] Copyright terms are being lengthened and some argue that fair use is being unduly contracted.[115] The right of publicity is growing to include any advertising, merchandising, and even interior decor that reminds people of a celebrity, even if it doesn't use the celebrity's name or likeness.[116]

Many have criticized this creeping propertization of speech, often on First Amendment grounds.[117] They have decried the tendency of many courts to merely label speech restrictions "property rules" as if such a relabeling could eliminate the First Amendment objections.[118] They have pointed out that cases upholding the propriety of some speech restrictions—such as the core of copyright law, traditional trademark law aimed at preventing consumer confusion, or the right to control the rebroadcast of one's entire act—don't necessarily validate all new restrictions that one might call "copyright," "trademark," or "right of publicity" (much less "intellectual property" generally).[119]

---

114. *See generally* Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L.J. 1687 (1999).

115. *See, e.g.*, Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996.

116. *See, e.g.*, White v. Samsung Elecs. Am., Inc., 989 F.2d 1512, 1520 (9th Cir.) (Kozinski, J., dissenting from denial of rehearing en banc); Wendt v. Host Int'l, 125 F.3d 806 (9th Cir. 1997); Madow, *infra* note 111; Zimmerman, *infra* note 220.

117. *See, e.g.*, Lemley, *supra* note 114, at 1710-12 ("The expansive power that is increasingly being granted to trademark owners has frequently come at the expense of freedom of expression. As trademarks are transformed from rights against unfair competition to rights to control language, our ability to discuss, portray, comment, criticize, and make fun of companies and their products is diminishing."); Litman, *supra* note 111 (arguing that expansions of copyright law and of other intellectual property rights pose First Amendment problems, and that even existing copyright law may sometimes impermissibly restrict speech); Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994) (same); Jessica Litman, *Copyright and Information Policy*, 55 LAW & CONTEMP. PROBS. 185, 204-05 (1992) (same); Malla Pollack, *The Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, The Intellectual Property Clause and The First Amendment*, 17 CARDOZO ARTS & ENT. L.J. 47 (1999) (arguing that proposed property rights in factual databases violate the First Amendment); Memorandum in Support of Plaintiff's Motion for Summary Judgment, Eldred v. Reno, No. 1:99CV00065 JLG), at 31-52, *available at* <http://cyber.law.harvard.edu/eldredvreno/legaldocs.html> (drafted primarily by Larry Lessig) (arguing that both the prospective and the retroactive extension of the copyright term violates the Free Speech Clause); Zimmerman, *supra* note 56, at 673 (arguing that "better principles for confining the sphere of property rules" are needed to prevent Free Speech Clause violations).

118. *See* note 56 *supra*.

119. *See, e.g.*, Zimmerman, *supra* note 56 (approving of properly bounded intellectual property law, but criticizing its recent expansion); Lemley, *supra* note 114 (approving of properly bounded trademark law, but criticizing its recent expansion); Malla Pollack, *Time to Dilute the Dilution Statute*, 78 J. OF PAT. AND TRADEMARK OFF. SOC'Y 519, 526-32 (1996) (same); Malla Pollack, *Your Image is My Image*, 14 CARDOZO L. REV. 1391, 1397-1448 (1993) (same); Alfred Yen, *A First Amendment Perspective on the Idea-Expression Dichotomy and Copyright in a Work's "Total Concept and Feel,"* 38 EMORY L.J. 393 (1989) (approving of properly bounded copyright law, but criticizing the vagueness of the standards established by some copyright cases); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998) (approving of properly bounded substantive intellectual property protections, but criticizing the use of certain remedies in intellectual property cases); Eugene Volokh & Brett

But if the arguments that "it's not a speech restriction, it's an intellectual property rule" or "the Supreme Court has upheld property rights in information, so property rights in information are constitutional" are accepted for information privacy speech restrictions, they will be considerably strengthened as to the other restrictions, too. If, for instance, courts hold that information privacy speech restrictions are proper because they merely "internalize th[e] cost" of their speech "by paying those whose data is used,"[120] it will be easy to argue the same as to other "data" that someone may say is his. Likewise, if courts hold that such speech restrictions are permissible because the restrictions encourage "a process of voluntary exchange, [that,] like the free market generally, would assure that 'human satisfaction as measured by aggregate consumer willingness to pay . . . is maximized,'" the same argument could apply to broad new rights in all sorts of information.[121]

Of course, courts already can, if they really want to, uphold new intellectual property rules by analogy to the existing old ones; but the creation of yet another kind of intellectual property speech restriction—and one that promises to be quite popular—will strengthen the argument. Ask yourself: Would the courts be less likely to accept the notion of property in personal information if trademark and right of publicity had never existed, and the only intellectual property speech restriction were copyright? Probably yes; there are too many distinctions between personal information and copyrightable expression for this one analogy to be that helpful. But as other potential analogies are added, the argument becomes easier—one can say "this proposal is sound because it's like precedent A in one respect, like precedent B in another respect, and like precedent C in a third respect," so even if the proposal is unlike any particular precedent, it can be seen by observers as similar to their aggregate. If this is so, then the case for new intellectual property speech restraints would be further strengthened by the recognition of yet one more kind of such speech restriction to which people can analogize.[122]

Moreover, as I've argued, a new exception for a property right in personal information would be the first (but I fear not the last) First Amendment authorization for a property right in pure facts. Right now the database protection proposals are being confronted with the objection that the law does *not* generally recognize intellectual property rights that restrict communica-

---

McDonnell, *Freedom of Speech and Independent Judgment Review in Copyright Cases*, 107 YALE L.J. 2431 (1998) (approving of properly bounded copyright law, but criticizing the way courts review copyright judgments).

120. Lessig, *supra* note 47, at 63.

121. Bloustein, *supra* note 48, at 439-40; *see also* Murphy, *supra* note 47, at 2395-96.

122. *See* note 227 *infra* (giving a real example of how existing intellectual property speech restrictions are used as arguments for creating new First Amendment exceptions).

tion of facts.[123] The analogy to copyright law actually works against those proposals, because they seek to protect exactly what the Court in *Feist Publications, Inc. v. Rural Telephone Service Co.*[124] said copyright doesn't protect, and they seek to do exactly what the Court in *Harper & Row* said would violate the First Amendment—use an "[intellectual property] monopoly as an instrument to suppress facts."[125] But if information privacy speech restrictions are upheld, they would provide an excellent new analogy for the database protection bill supporters. The same is true for the asserted right to property in hot news, which is today subject to powerful free speech attack,[126] but which would be strengthened if the courts accept another property right in facts.

Now perhaps my parade of horribles isn't so horrible; maybe we should have more property rights in facts, which is to say restrictions or speech that communicates facts. Or if I am right to be skeptical of such new property rights, perhaps supporters of property rights in personal information can come up with a narrow justification for those particular rights that will provide little precedential support for the other proposals. Nonetheless, people who are worried about the general trend towards propertization of information should look very carefully at even those proposals that might at first seem benign and even just; such proposals could have effects far beyond the context in which they are first suggested.

IV. COMMERCIAL SPEECH

A. *What "Commercial Speech" Means*

Some argue that sale of information about customers is restrictable because it fits within the "commercial speech" doctrine.[127] The Court's definition of "commercial speech," though, isn't (and can't be) simply speech that

123. *See, e.g.*, Memorandum from William Michael Treanor, U.S. Department of Justice Office of Legal Counsel, to Office of Deputy Assistant Attorney General (July 28, 1998), *available at* <http://www.itaa.org/govt/legact/dbdoj.htm> (discussing constitutional concerns about collections of Information Antipiracy Act); Pollack, *supra* note 117; Benkler, *supra* note 111; J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997).

124. 499 U.S. 340 (1991).

125. Harper & Row v. Nation Enter., 471 U.S. 539, 559 (1985).

126. *See, e.g.*, Zimmerman, *supra* note 56, at 719-23, 726-27, 733; RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 cmts. b & c (largely rejecting the concept of a property right in hot news and criticizing International News Service v. Associated Press, 248 U.S. 215 (1918), which pioneered that right).

127. *See, e.g.*, United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133, 1137 (9th Cir. 1999), *rev'd on other grounds sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999); Cohen, *supra* note 10, at 1409-16 (analyzing information privacy speech restrictions only under commercial speech doctrine, though acknowledging that personally identifiable information, even when sold, might not in fact qualify as "commercial speech").

is sold as an article of commerce: Most newspapers, movies, and books are articles of commerce, too, but they remain fully protected.[128] Likewise, speech can't be commercial just because it relates to commerce, or else the *Wall Street Journal,* union leaflets and newsletters,[129] newspaper reviews of commercial products,[130] and speech by disgruntled consumers criticizing what they consider poor service by producers[131] would be deprived of full constitutional protection.

Rather, the Court's most common definition of commercial speech is speech that explicitly or implicitly "propose[s] a commercial transaction."[132] Commercial advertisements for products or services are classic examples. So are stock prospectuses, which propose the purchase of stock; this is why fairly heavy SEC regulation of speech in such prospectuses is largely permissible, while similar SEC regulation of newsletters or newspapers that discuss stocks is not.[133] At the outer boundary, a company's publications that generally discuss a kind of product without mentioning the company by name—for instance, a contraceptive producer's pamphlets discussing contraception generally, rather than just the producer's own devices—also qualify as commercial speech.[134] Query, though, how far this goes: It's not clear, for instance, that a book touting the health benefits of wine should be treated differently depending on whether its author owns a leading winery.

The Court has at times suggested that the commercial speech category may also generally cover speech that is "related solely to the economic interests of the speaker and its audience,"[135] and some lower courts have accepted this definition.[136] But this can't be right. Consider again the newspaper that

---

128. *See, e.g.*, Smith v. California, 361 U.S. 147, 150 (1959) ("It is of course no matter that the dissemination [of speech by the claimant] takes place under commercial auspices"); Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501 (1952) ("It is urged that motion pictures do not fall within the First Amendment's aegis because their production, distribution, and exhibition is a large-scale business conducted for private profit. We cannot agree. That books, newspapers, and magazines are published and sold for profit does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment."). Suggestions that information privacy speech restrictions are permissible because they merely involve "the market exchange of information for value" or "information . . . as (owned and traded) commodity," *see, e.g.*, Cohen, *supra* note 10, at 1376, 1414, thus seem to me unsound: Communication of information is constitutionally protected even when it's done for money in the marketplace.

129. *See, e.g.*, Debartolo Corp. v. Florida Gulf Coast Trades Council, 485 U.S. 568 (1988).

130. *See, e.g.*, Bose Corp. v. Consumers Union, 466 U.S. 485 (1984).

131. *See* notes 149-154 *infra* and accompanying text.

132. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 761 (1976).

133. *See* Lowe v. SEC, 472 U.S. 181, 211 (1985) (White, J., concurring in the judgment).

134. Bolger v. Youngs Drug Products Corp., 463 U.S. 60 (1983).

135. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 561 (1980).

136. *See, e.g.*, Hoover v. Morales, 164 F.3d 221, 225 (5th Cir. 1998); United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133, 1136-37 (9th Cir. 1998) (appearing to endorse this test, though not explicitly applying it), *rev'd on other grounds sub nom.* Los Angeles

discusses business affairs, almost entirely in order to make money by helping its readers do well in business. Consider a product review written by its author because he wants to be paid, published by the newspaper because it wants to keep its paying subscribers, and read by readers because they want to know how to best spend their money. Consider a union buying TV ads urging people to "Buy American" because that's the best way of maintaining the viewers' (and the union members') standard of living.

Such economic commentary, it seems to me, is as protected as political, religious, social, or artistic commentary. That it has to do with the listeners' economic interests merely highlights its importance—for most people, economic well-being is more important than politics, art, social concerns, or often even religion, and speech on economic matters often has more effect on the nation than does most art or theology, or even much political debate. The speech may not be "political" in the narrow sense of the word, but (as I discuss further in Part IV), the Court has long recognized that strong First Amendment protection extends far beyond politics. Nor does the speech implicate the concerns about fraud in a particular commercial transaction that have been seen as justifying the regulation of commercial *advertising*. In fact, every one of the Court's dozens of commercial speech cases has involved speech that advertises a product or service;[137] and the last decade's precedents, which have generally been shifting in the direction of more protection even for speech that is classified as "commercial speech," have stressed the "proposes a commercial transaction" formulation and largely ignored the "solely economic interests" test.[138]

Under the "speech that proposes a commercial transaction" analysis, communication of information about customers by one business to another is not commercial speech. It doesn't advertise anything, or ask the receiving business to buy anything from the communicating business.[139] It poses no special risk of the speaker misleading or defrauding the listener, beyond those risks present with fully protected speech generally. The recipient busi-

---

Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999); Abramson v. Gonzalez, 949 F.2d 1567, 1574 (11th Cir. 1992).

137. One of those cases, *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60 (1983), involved indirect advertising.

138. *See, e.g.*, 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 504 (1996) (referring to the "proposes a commercial transaction" formula without referring to the "solely economic interests" formula); City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 421 (1993) (stressing that the Court has been shifting away from the "economic interests" formulation and towards the "proposes a commercial transaction" formulation); Rubin v. Coors Brewing Co., 514 U.S. 476, 482 (1995) (same); United States v. Edge Broadcasting Co., 509 U.S. 418 (1993) (same); Edenfield v. Fane, 507 U.S. 761 (1993) (same).

139. Sometimes, of course, a business will use customer information that it has bought from another business to send out commercial advertisements to prospective clients. These advertisements would indeed be commercial speech, though the original communication of the customer information is not. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

ness does intend to use the information to more intelligently engage in commercial transactions, but that's equally true of businesspeople reading *Forbes*.[140]

Some might argue that there's something inherently un-speech-like in corporations communicating to other corporations, but there's no reason why this would be so. To begin with, the corporate status of the speaker or the listener can't be relevant; surely it can't matter for privacy purposes whether customer information is communicated by and to corporations, partnerships, or sole proprietorships. And the Court has specifically held that speech doesn't lose its constitutional protection because the speaker is a corporation,[141] which makes sense for various reasons, among them that almost all media organizations and many nonprofit political advocacy groups are corporations.

Even if we recast the claim as focusing on businesses communicating to other businesses, the fact is that businesses don't communicate—people communicate. When the managers of Acme Software, at their CEO's urging, read the *Wall Street Journal* so they can apply what they learn to their business decisions, this isn't "the *Wall Street Journal* communicating to Acme." It's people at the *Journal*—the editors, who direct the creation of a joint product by many writers—communicating to people who run Acme. When a scientist working in industry sends the results of his experiments to another scientist also working in industry, the communication may be said to be between their employers (since for both scientists it's part of their jobs), but it's also between people. Likewise, it is no less speech when a credit bureau sends credit information to a business. The owners or managers of a

---

140. *Accord* The U.D. Registry, Inc. v. California, 40 Cal. Rptr. 2d 228, 230 (Ct. App. 1995):

> The test for identifying commercial speech is whether the expression at issue proposes a commercial transaction. Applying this settled definition, it is clear that the expression in this case, truthful information taken from public records regarding unlawful detainer defendants, does not propose a commercial transaction, and hence is not commercial speech. The fact that UDR sells the information does not transform it to commercial speech any more than the fact that a magazine or newspaper is sold makes its contents commercial speech.

See, e.g., Shorr, *supra* note 98, at 1798-1812 (discussing this question in great detail). *United Reporting Publ'g Corp. v. California Highway Patrol* took the contrary view, concluding that "United Reporting sells arrestee information to clients; nothing more. Its speech can be reduced to, 'I [United Reporting] will sell you [client] the X [names and addresses of arrestees] at the Y price.' This is a pure economic transaction, comfortably within the 'core notion' of commercial speech." 146 F.3d 1133, 1136 (9th Cir. 1998) (alterations in original), *rev'd on other grounds sub nom.* Los Angeles Police Department v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999). This, though, is mistaken—just as the fact that the *New York Times* sells information to subscribers at a certain price doesn't make the *Times* commercial speech, so the fact that United Reporting sells information to clients at a certain price doesn't make its speech commercial. The Ninth Circuit's argument may support the notion that United Reporting's *offer* to its customers to sell them information is commercial speech; but the state statute in that case restricted the communication of the information, not the offer to communicate it.

141. First Nat'l Bank v. Bellotti, 435 U.S. 765 (1978).

credit bureau are communicating information to decisionmakers, such as loan officers, at the recipient business.[142]

It's true that in such cases, neither the speaker nor the listener intend to communicate an ideological message through the information, but that's just because the information is fact, not idea. Likewise, in many such cases, neither the speaker nor the listener sees this factual communication as implementing or furthering some ideology, in part because it's just their job. In some cases, though, the people *will* see the communication as a means of implementing some ideology—"we report the news because the truth is sacred," "we make the wheels of business run more smoothly," "we want to advance the progress of science," "we help protect you from deadbeats because failure to repay a loan is a form of fraud that we want to stop." Many businesspeople genuinely believe that their work is not just a job but part of a broader mission to improve society; it's a peculiar conceit of some professional would-be opinion molders to think that they alone really believe in what they're doing, and that everyone else is only in it for the money. I suspect that the ideological commitment of a typical newspaper reporter who's writing, say, product reviews or local crime stories is not much different from the ideological commitment of a typical businessperson. And this fact helps explain why speech is protected without regard to the speaker's or the listener's ideological motivations.

Of course, even if speech that communicates personal information is seen as "commercial speech," restrictions on such speech will still have to face considerable scrutiny. Whether they will pass such scrutiny is hard to tell, since commercial speech scrutiny is so notoriously vague.[143] But this question is actually somewhat tangential to my main point. To me, the main problem with treating speech that communicates personal information as "commercial speech" is not that this will put such speech at more risk of restriction. Rather, it is that stretching the definition of "commercial speech" will put a wide range of other speech at risk, too.

B. *The Risks to Other Speech*

Consider a recent example of the government trying to regulate cyberspace speech about economic matters on the grounds that it's "commercial speech." In *Taucher v. Born,* several operators of commodities-themed Web

142. *See* Dun & Bradstreet v. Greenmoss Builders, 472 U.S. 749 (1985) (treating such business-to-business communication as speech subject to First Amendment protection, though concluding that false statements of fact on matters of private concern are subject to presumed and punitive damages despite the First Amendment).

143. *Cf.* United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998) (striking down such a restriction even under commercial speech scrutiny), *rev'd on other grounds sub nom.* Los Angeles Police Department v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999).

sites successfully sued to set aside a prior restraint system which bars people from distributing for profit any unlicensed speech that relates "to the value of or the advisability of commodity trading" or that contains "analyses or reports" about commodities.[144] And the license that speakers must get to be allowed to speak isn't just a modest tax; the Commodities Futures Trading Commission can refuse a license if it finds "good cause" to do so, and speaking without a license is illegal. Nor is this speech restriction limited to individualized, person-to-person professional advice: The regulation is broad enough to cover people who "never engage in individual consultations with their customers" and who "under no circumstances make trades for their customers."[145]

The law essentially restricts the Web equivalent of books and newspapers about commodity training—it's as if the government claimed the right to refuse the *Wall Street Journal* a license to publish articles about the market. As it happens, the law specifically excludes publishers who publish such data "incidental[ly]" as part of a broader news enterprise of "general and regular dissemination,"[146] so the *Journal* can sleep easy—and the CFTC can sleep easy without the risk of incurring the ire of established, powerful news organs. But under the logic of the law, newspapers and book publishers could also be subject to a prior restraint system, just as the small commodities-focused electronic publishers were subject to it until the court's ruling.

The CFTC argued that speech about commodities is mere "commercial speech," but the court correctly rejected this:[147] "The plaintiffs' publications in this case do not propose any commercial transaction between the plaintiffs and their customers."[148] If, however, the commercial speech doctrine had been extended to cover the sale of speech about a business's clients, the court's decision might well have been different. After all, the Web business journalist who writes about commodities is likewise selling information that's primarily of economic concern, and that has little to do with broad political debates. If that's enough to deny free speech protection to communications about customers, it may be enough to deny such protection to communications about commodities.

144. 7 U.S.C. § 6m(1).

145. Taucher v. Born, 53 F. Supp. 464, 478 (D.D.C. 1999).

146. 7 U.S.C. §§ 1a(5)(B)(iv), 1a(5)(C).

147. The CFTC's other argument was that the government may regulate speech in the context of a professional-client relationship, but the court adopted the response to a similar argument given by Justice White in his *SEC v. Lowe*, 472 U.S. 181 (1985), concurrence: Whatever extra power the government may have to regulate the professional-client relationship, this power arises only when the professional exercises individualized judgment on behalf of a particular client. Personal advice may to some extent be restricted, but books, newsletters, and the like may not be.

148. *Taucher v. Born*, 53 F. Supp. at 480.

Consider another example: disgruntled homebuyers putting up signs criticizing the developer that sold them their homes, or consumers leafleting outside a business that they claim sold them defective goods, often hoping that the business will give them a refund or at least will do a better job in the future. In cyberspace, the analogy would be consumers putting up a *http://www.[businessname]sucks.com* site or circulating messages to a long list of acquaintances or to a Usenet newsgroup.

In my view, the First Amendment fully protects such speech that is aimed at creating public pressure on someone to do what you think is right, even in economic contexts—that, after all, is what much advocacy is about.[149] The fact that the speech exposes alleged problems with a product and aims at redressing an economic harm should not strip it of protection. Again, for many people problems with their homes and redress for shoddy wares are more important than problems with politicians and redress for shoddy policies, and far more important than art, entertainment, or many other kinds of fully protected speech.

If the consumer's speech is an intentional lie (or perhaps in some circumstances if it's merely negligently false), the business can sue for libel; false statements of fact, whether on economic matters or not, lack constitutional protection.[150] But the law shouldn't impose extra restrictions on the speech just because the speech deals with economic issues. It shouldn't, for instance, punish true speech on the grounds that it interferes with a business's prospective economic advantage.[151] It shouldn't impose prior restraints such as preliminary injunctions on the speech, even if the court

149. *See, e.g.*, Debartolo Corp. v. Florida G. Coast Trades Council, 485 U.S. 568 (1988); NAACP v. Claiborne Hardware, 458 U.S. 886 (1982); Keefe v. Organization for a Better Austin, 402 U.S. 415 (1971) ("The claim that the expressions were intended to exercise a coercive impact on respondent does not remove them from the reach of the First Amendment. Petitioners plainly intended to influence respondent's conduct by their activities; this is not fundamentally different from the function of a newspaper. Petitioners were engaged openly and vigorously in making the public aware of respondent's real estate practices. Those practices were offensive to them, as the views and practices of petitioners are no doubt offensive to others. But so long as the means are peaceful, the communication need not meet standards of acceptability.").

150. *See, e.g.*, Bose Corp. v. Consumers Union, 466 U.S. 485 (1984) (assuming that the standards for trade libel lawsuits are the same as for libel lawsuits); Turf Lawnmower Repair, Inc. v. Bergen Record Corp., 139 N.J. 392, 412 (1995) (establishing a standard for trade libel lawsuits that is similar to that for libel lawsuits, with distinctions drawn between small stores that are treated as private figures and may recover actual damages on a showing of negligence, and large or heavily regulated businesses that are treated as public figures and must show actual malice).

151. *See, e.g.*, Paradise Hills Assocs. v. Procel, 1 Cal. Rptr. 2d 514, 521, 523 (Ct. App. 1991) (describing and rejecting the claim that speech interfering with prospective economic advantage and "involv[ing] solely private issues rather than matters of public concern" may be enjoined even if it is true); Springfield Bayside Corp. v. Hochman, 255 N.Y.S.2d 140 (1964) (enjoining tenant picketing of landlord, even assuming that the tenants' allegations were true); Saxon Motor Sales, Inc. v. Torino, 2 N.Y.S.2d 885 (1938) (enjoining a car buyer from parking his car in front of the car dealership with a sign alleging that the car is a lemon, without regard to whether the allegations were true).

tentatively concludes that the speech is probably false.[152] And even if the speech is found to be in error, the law shouldn't impose liability unless some fault on the speaker's part is shown. Though some such speech restrictions may be permissible as to commercial speech,[153] they're not permissible as to noncommercial speech; and under current doctrine, consumer criticisms aren't commercial speech because they don't propose a commercial transaction between the speaker and the listener.[154]

Again, though, a broadening of the commercial speech doctrine would jeopardize speech of this sort. If communicating information about a person's bad credit record is mere "commercial speech," then communicating information about a business's bad service record should be, too. Both, after all, involve speech on economic matters. Both involve speech that's primarily of economic interest to listeners. Both are motivated by the speaker's economic interest—either a desire to get money from the buyer of the information, or a desire to get redress from the business. Either both are commercial speech or neither is.

In a free and competitive economy, people naturally want to talk about economic matters. Often their motives for such speech are largely economic: They want to learn how to make more money. They want to persuade people that some course of action is economically better. They want to alert people to what they think are others' dishonest business practices. Giving the government an ill-defined but potentially very broad power to restrict such speech—not just speech that proposes a commercial transaction between speaker and listener and thus directly implicates the risk of fraud—risks exposing a great deal of speech to government policing.[155]

---

152. *See generally* Lemley & Volokh, *supra* note 119, at 169-78.

153. *See* U.S. Healthcare, Inc. v. Blue Cross of Greater Philadelphia, 898 F.2d 914, 937 (3rd Cir. 1990) (holding that a libel lawsuit brought by a public figure plaintiff based on a statement about a matter of public concern could succeed without a showing of either actual malice or negligence, because the statement was in a commercial ad and was therefore commercial speech); Friedman v. Rogers, 440 U.S. 1, 10 (1979) (suggesting that the prohibition on prior restraints may be inapplicable to commercial speech cases); Virginia State Bd. of Pharmacy v. Virginia Citizens' Consumer Council, 425 U.S. 748, 772 n.24 (1976) (same); Kleiner v. First Nat'l Bank of Atlanta, 751 F.2d 1193, 1203-05 (11th Cir. 1985) (interpreting *Friedman* and *Virginia Pharmacy* as meaning that "commercial speech seldom implicates the traditional concerns underlying the prior restraint doctrine").

154. *See, e.g., Paradise Hills Assocs.*, 1 Cal. Rptr. 2d at 522 ("Nor is [Procel's] speech merely commercial speech which is entitled to less protection under the First Amendment. 'The test for identifying commercial speech is whether the publication in question may be said to do no more than 'propose a commercial transaction.'' Procel's speech does not meet that test." (citations omitted)).

155. Some defenses of information privacy speech restrictions would potentially go even further towards dramatically transfiguring free speech principles. (I say "potentially" because these arguments are generally fairly abstract, so their exact scope is often impossible to predict.)

Consider, for instance, the argument that Congress should be able to restrict communication of information about consumers "to prevent the systemic, structural consequences of a growing imbal-

V. SPEECH ON MATTERS OF PRIVATE CONCERN

A. *The Argument*

One feature of virtually all information privacy proposals (except those built on a contract model) is their distinction between speech on matters of public concern and speech on matters of private concern.[156] Even people who argue that newspapers should be forbidden from publishing a private person's long-ago criminal history or a politician's sexual orientation would probably agree that they have a right to publish the politician's criminal history, no matter how old. Warren and Brandeis would have called this a "matter which is of public or general interest";[157] others call it "political speech" or "speech on matters of public concern" or "newsworthy" material.

---

ance of informational power." Cohen, *supra* note 10, at 1415. The argument is referring to a supposed imbalance of "informational power" between vendors and consumers, but it would apply even more strongly to the imbalance of power between the public and the media: The media, being in the information business, necessarily have much more information and the power that flows from it than consumers do. If such imbalances of power, which of course have been around as long as the organized press, were reason enough to suppress speech on certain topics, then Congress would finally be able to pervasively regulate what newspapers, magazines, and Web sites discuss—and with a populist, egalitarian justification to boot. *Cf., e.g.*, Richard L. Hasen, *Campaign Finance Laws and the Ruport Murdoch Problem*, 77 TEX. L. REV. 1627, 1627, 1631, 1634 (1999) (arguing that "media consolidation" and concerns about "equality" justify, among other things, restrictions on newspaper editorials that "endors[e] or oppose[e] candidates").

Likewise for the argument that the need to "promot[e] individual autonomy and self-determination" justifies "Congress . . . regulat[ing] data processing practices," including communication of information about people, "that seek to reduce individuals to the objects of commercial preference-manipulation:" Cohen, *supra* note 10, at p.35. Speakers, of course, try to manipulate our preferences all the time. Music videos try to make us think that certain bands are cool. Calls for boycotts try to manipulate buyers and, even more powerfully, the boycott targets. *See, e.g.*, NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982) (rejecting claim by business affected by boycott that boycott organizers should be liable for the boycott's economic effects); Organization for Better Austin v. Keefe, 402 U.S. 415 (1971); note 235 *infra*. And of course the whole point both of editorials and subtle political spin in news stories is to "manipulat[e]" our political preferences. If speech is constitutionally protected even if it "intend[s] to influence [people's] conduct" by threat of boycott or social ostracism, *Organization for Better Austin*, 402 U.S. at 419, or by partisan shading of the facts, then it's hard to see why it should become unprotected just because its recipients plan to use it to influence consumers' buying habits. Conversely, once the legislative desire to prevent "preference manipulation" becomes a justification for restricting speech on certain subjects, such a justification could be easily applied to a wide variety of speech that some see as "manipulat[ive]."

156. *See, e.g.*, among many others, Edelman, *infra* note 268, at 1229-30; Cohen, *supra* note 10, at 1414, 1417 (concluding that personally identifiable data is "not a vehicle for injecting communication into the 'marketplace of ideas'" but is rather "a tool for processing people," and ultimately concluding that therefore "a lesser level of scrutiny is warranted"); *id.* at 1417, 1418 (going so far as to suggest that "we need not apply first amendment standards of review at all" where collections of personally identifiable data are concerned, because "in the ways that matter [such communication isn't] really 'speech' at all").

157. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214 (1890). Warren and Brandeis didn't confront exactly this example, but they did say that "publish[ing] of a modest and retiring individual that he suffers from an impediment in his speech or that

Speech that fits within these labels, they would argue, is constitutionally protected, while speech that is merely of private concern is not protected, at least against information privacy speech restrictions. But this approach, I will argue, is theoretically unsound; it is precedentially largely unsupported; in the few circumstances in which it has been endorsed, it has proven unworkable; and, if adopted, it would strengthen the arguments for many other (in my view improper) speech restrictions.

B. *Theoretical Objections*

Under the First Amendment, it's generally not the government's job to decide what subjects speakers and listeners should concern themselves with.[158] A private concern exception essentially says "you have no right to speak about topics that courts think are not of legitimate concern to you and your listeners," a view that's inconsistent with this understanding.[159]

A clear example of the danger of such government power comes in a disclosure tort case, *Diaz v. Oakland Tribune*.[160] Diaz, the first woman student body president at a community college, was a transsexual, and the Oakland Tribune published this fact. Diaz sued, and the court of appeals held that her lawsuit could go forward; if a jury found that Diaz's transsexuality wasn't newsworthy, she could prevail.[161] As usually happens in these cases, the court didn't define newsworthiness but left it to the jury, subject only to the instruction that "[i]n determining whether the subject article is newsworthy you may consider [the] social value of the fact published, the depth of the article, [its] intrusion into ostensibly private affairs, and the extent to which the plaintiff voluntarily acceded to a position of public notori-

---

he cannot spell correctly, is an unwarranted . . . . infringement of his rights, while to state and comment on the same characteristics found in a would-be congressman could not be regarded as beyond the pale of propriety." *Id.* at 215.

158. *See, e.g.*, Police Dep't v. Mosley, 408 U.S. 92, 95 (1972) ("[A]bove all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."). The Court has recognized some exceptions to this principle, but this presumption is still the basis for the Court's analysis of speech restrictions imposed by the government as sovereign.

159. *Cf.* Rosenbloom v. Metromedia, Inc., 403 U.S. 29, 44 (1971) (Marshall, J., dissenting) ("[A]ssuming that . . . courts are not simply to take a poll to determine whether a substantial portion of the population is interested or concerned in a subject, courts will be required to somehow pass on the legitimacy of interest in a particular event or subject [and thus on] what information is relevant to self-government. . . . The danger such a doctrine portends for freedom of the press seems apparent."); Cynthia L. Estlund, *Speech on Matters of Public Concern: The Perils of an Emerging First Amendment Category*, 59 GEO. WASH. L. REV. 1, 30 (1990); Robert Post, *The Constitutional Concept of Public Discourse*, 103 HARV. L. REV. 603, 670-79 (1990). Estlund's and Post's pieces are classics in the field. *See also* Cynthia L. Estlund, *Freedom of Expression in the Workplace and the Problem of Discriminatory Harassment*, 75 TEX. L. REV. 687, 753 (1997).

160. 188 Cal. Rptr. 762 (Ct. App. 1983).

161. The court set aside the verdict for Diaz because of a jury instruction error, but remanded for a new trial.

ety."[162] But the court did stress that a jury could find that the speech wasn't newsworthy: "[W]e find little if any connection between the information disclosed and Diaz's fitness for office. The fact that she is a transsexual does not adversely reflect on her honesty or judgment."[163]

Now I agree with the court's factual conclusion; people's gender identity strikes me as irrelevant to their fitness for office. But other voters take a different view. Transsexuality, in their opinion, may say various things about politicians (even student body politicians): It may say that they lack attachment to traditional values, that they are morally corrupt, or even just that they have undergone an unnatural procedure and therefore are somehow tainted by it. These views may be wrong and even immoral, but surely it is not for government agents—whether judges or jurors—to dictate the relevant criteria for people's political choices, and to use the coercive force of law to keep others from informing them of things that they may consider relevant to those choices.[164] I may disagree with what you base your vote on, but I must defend your right to base your vote on it, and the right of others to tell you about it.

This is the clearest example of a court using the public concern test to usurp what should be a listener's and speaker's choice, but other public disclosure cases raise similar problems. Consider, for instance, the criminal history cases, in which some courts held that it was illegal for newspapers to print information about "long past" criminal activity by people who are now supposedly rehabilitated and are leading allegedly blameless lives. The leading such case is *Briscoe v. Reader's Digest Association,* in which *Reader's Digest* was held liable for revealing that Briscoe had eleven years earlier been convicted of armed robbery (a robbery that involved his fighting "a gun battle with the local police").[165]

---

162. *Id.* at 770 n.15.

163. *Id.* at 773; *cf.* Warren & Brandeis, *supra* note 157, at 216 (urging the "repress[ion]" of revelations that "have no legitimate connection with [a person's] fitness for a public office which he seeks or for which he is suggested").

164. Peter Edelman suggests, as to a somewhat different hypothetical, that "[p]erhaps a useful idea with regard to newsworthiness is that the media may not rely on satisfying popular prejudices as a justification for a news decision," Edelman *infra* note 268, at 1229, and some might argue that this should apply to the *Diaz* case. It seems to me, though, that whatever power the courts may have to set aside government action that is based on or gives effect to people's prejudices—Edelman cites one such case, *Palmore v. Sidoti,* 466 U.S. 429, 434 (1984), as support for his argument—the courts have no business deciding whether a voter's potential decision about a candidate is "prejudice[d]" or not. In a democratic government, it is for the voters to pass judgment on government officials' reasons for action, not for government officials to restrict speech in order to control voters' reasons for action.

165. 483 P.2d 34, 36 (Cal. 1971); *see also* Melvin v. Reid, 297 P. 91 (Cal. Ct. App. 1931) (involving the revelation that an upstanding citizen had been a prostitute and an alleged murderer seven years earlier); Roshto v. Hebert, 413 So. 2d 927 (La. Ct. App. 1982) (involving the republication of the 25-year-old front page of a newspaper, which contained an article describing plaintiffs' cattle theft convictions).

The court acknowledged that the speech, while not related to any particular political controversy, was newsworthy; the public is properly concerned with crime, how it happens, how it's fought, and how it can be avoided.[166] Moreover, revealing the identity of someone "currently charged with the commission of a crime" is itself newsworthy, because "it may legitimately put others on notice that the named individual is suspected of having committed a crime,"[167] thus presumably warning them that they may want to be cautious in their dealings with him.

But revealing Briscoe's identity eleven years after his crime, the court said, served no "public purpose" and was not "of legitimate public interest"; there was no "reason whatsoever" for it.[168] The plaintiff was "rehabilitated" and had "paid his debt to society."[169] "[W]e, as right-thinking members of society, should permit him to continue in the path of rectitude rather than throw him back into a life of shame or crime" by revealing his past.[170] "Ideally, [Briscoe's] neighbors should recognize his present worth and forget his past life of shame. But men are not so divine as to forgive the past trespasses of others, and plaintiff therefore endeavored to reveal as little as possible of his past life."[171] And to assist Briscoe in what the court apparently thought was a worthy effort at concealment, the law may bar people from saying things that would interfere with Briscoe's plans.

Judges are of course entitled to have their own views about which things "right-thinking members of society" should "recognize" and which they should forget; but it seems to me that under the First Amendment members of society have a constitutional right to think things through in their own ways. And some people do take a view that differs from that of the *Briscoe* judges: While criminals can change their character, this view asserts, they often don't. Someone who was willing to fight a gun battle with the police eleven years ago may be more willing than the average person to do something bad today, even if he has led a blameless life since then (something that no court can assure us of, since it may be that he has continued acting violently on occasion, but just hasn't yet been caught).

Under this ideology, it's perfectly proper to keep this possibility in mind in one's dealings with the supposedly "reformed" felon. While the government may want to give him a second chance by releasing him from prison, restoring his right to vote and possess firearms, and even erasing its publicly accessible records related to the conviction, his friends, acquaintances, and business associates are entitled to adopt a different attitude. Most presuma-

166. 483 P.2d at 40.
167. *Id.* at 39.
168. *Id.* at 40, 43.
169. *Id.* at 37, 41.
170. *Id.* at 41 (quoting and endorsing Melvin v. Reid, 297 P. 91, 93 (Cal. Ct. App. 1931)).
171. *Id.* at 41-42.

bly wouldn't treat him as a total pariah, but they might use extra caution in dealing with him, especially when it comes to trusting their business welfare or even their physical safety (or that of their children) to his care.[172] And, as Richard Epstein has pointed out, they might use extra caution in dealing with him precisely because he has for the last eleven years hidden this history and denied them the chance to judge him for themselves based on the whole truth about his past.[173] Those who think such concealment is wrong will see it as direct evidence of *present* bad character (since the concealment was continuing) and not just of past bad character.

Revealing Briscoe's name, under this view, may have little to do with broad political debates, but it is still of intense and eminently legitimate public concern to one piece of the public: people who know Briscoe, the very same group whose ignorance Briscoe seemed most concerned about preserving.[174] These members of the public would use this information to make the decision, which is probably more important to them than whom they would vote for next November, about whether they could trust Briscoe in their daily dealings.

This isn't speech on political matters, but rather on what I might call "daily life matters." Under the First Amendment, which protects movies, art, jokes, and reviews of stereo systems,[175] such speech on daily life matters is at

---

172. If you were deciding whether to leave your children for the day in a neighbor's care, would you consider his eleven-year-old conviction for a violent crime involving a gun battle with police relevant (not necessarily dispositive, but relevant) to your decision? Would you advise your daughter to consider a prospective date's armed robbery conviction when deciding whether and under what conditions to go out with him?

173. Richard A. Epstein, *Privacy, Property Rights, and Misrepresentations*, 12 GA. L. REV. 455, 472-73 (1978).

174. *Briscoe*, 483 P.2d at 36 ("As the result of defendant's publication, plaintiff's 11-year-old daughter, as well as his friends, for the first time learned of this incident. They thereafter scorned and abandoned him.").

175. *See, e.g.*, Winters v. New York, 333 U.S. 507 (1948) (same as to entertainment); Bose Corp. v. Consumers Union, 466 U.S. 485 (1984) (treating product review of stereo equipment as fully protected); Abood v. Detroit Bd. of Educ., 431 U.S. 209, 231 (1977) ("[O]ur cases have never suggested that expression about philosophical, social, artistic, economic, literary, or ethical matters—to take a nonexhaustive list of labels—is not entitled to full First Amendment protection.").

Some argue that First Amendment doctrine should be dramatically revised so that only speech that is directly relevant to self-government would be constitutionally protected. Thus, for instance, Bloustein, *infra* note 179, takes an explicitly Meiklejohnian view that speech is protected only if it's relevant to self-government, and concludes that much personal information can therefore be suppressed. Meiklejohn's own experience with such a test, though, should sound a note of caution: Meiklejohn originally articulated this as a narrow standard that seemed to demand some serious connection of the speech to particular political questions; when people pointed out that this might deny protection to discussions of art, literature, science, and society, Meiklejohn revised his test to one that demanded a far looser connection to self-government, which ensured protection for literature but only at the expense of making the category virtually all-inclusive and thus doctrinally useless. *See, e.g.*, Estlund, *Speech on Matters of Public Concern*, *supra* note 159, at 45 (describing Meiklejohn's migration). In any event, today's First Amendment law is definitely not limited to Meiklejohn's original vision.

least equally worthy. At least as much as those kinds of protected speech, daily life matter speech—communication related to "the real, everyday experience of ordinary people"[176]—indirectly but deeply affects the way we view the world, deal with others, evaluate their moral claims on us, and even vote; and its effect is probably greater than that of most of the paintings we see or the editorials we read. Consider how much our view of crime and punishment, secrecy and publicity, and many other topics would be indirectly influenced—towards greater liberalism, conservatism, or something else—by the knowledge that some of our seemingly law-abiding neighbors have been concealing a criminal past.[177]

In any event, which viewpoint about our neighbors' past crimes is "right-thinking" and which is "wrong-thinking" is the subject of a longstanding moral debate. Surely it is not up to the government to conclude that the latter view is so wrong, that Briscoe's conviction was so "[il]legitimate" a subject for consideration, that the government can suppress speech that undermines its highly controversial policy of forgive-and-forget. I can certainly see why all of us might want to suppress "information about [our] remote and forgotten past[s]" in order "to change . . . others' definitions of [ourselves]."[178] But in a free speech regime, others' definitions of me should primarily be molded by their own judgments, rather than by my using legal coercion to keep them in the dark.[179]

The same goes for databases of personal information as much as for news stories about such information. Many such databases—for instance,

176. Estlund, *Speech on Matters of Public Concern*, *supra* note 159, at 37.

177. *See id.* at 38 n.220; Post, *supra* note 159, at 674; *cf.* STEVEN SHIFFRIN, THE FIRST AMENDMENT, DEMOCRACY, AND ROMANCE 48 & n.12 (1990) (citing evidence that voters assess the character of candidates "based in large part upon experiences with others in private life and on values formed through communications about other individuals in private life").

178. Fried, *supra* note 1, at 485 n.18 (crediting Erving Goffman with this argument).

179. Even if the story is seen as newsworthy only because it informs the public about crime (and even the *Briscoe* court acknowledged that the story was newsworthy in this sense), including the criminal's name still serves the important purpose of helping assure the public about the story's credibility. We all know how much easier it is to slant the presentation, omit important details, and even fudge the facts in stories that can't be corroborated; and when we see a story that we know can't be corroborated, we are naturally suspicious of it (and the behavior of journalists, fallible humans that they are, sometimes confirms the wisdom of such suspicion). True, few readers will personally check newspaper stories even if all the facts are given, but they know that the journalists know that such facts *could* be checked: A rival news organization, or a reader with personal knowledge of the details, can call them on their error. If the story omits the necessary details, people will quite properly discount its accuracy. *Cf.* Howard v. Des Moines Register & Tribune Co., 283 N.W.2d 289, 303 (Iowa 1979) ("[A]t a time when it was important to separate fact from rumor, the specificity of the report would strengthen the accuracy of the public perception of the merits of the controversy"); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 356 (1983) ("A factual report that fails to name its sources or the persons it describes is properly subject to serious credibility problems."). *But see* Edward J. Bloustein, *The First Amendment and Privacy: The Supreme Court Justice and the Philosopher*, 28 RUTGERS L. REV. 41, 93 (1974) (taking the opposite view).

credit history databases or criminal record databases—are used by people to help them decide whom it is safe to deal with and who is likely to cheat them. Other databases, which contain less incriminating information, such as a person's shopping patterns, may be less necessary for self-protection; but of course for the same reason the data stored in them will also generally be much less embarrassing to their subjects, which makes the supposed harm to the subjects of the communication of such data much smaller. And in any event, even this data is of direct daily life interest to its recipients, since it helps them find out with whom they should do business.

In some instances, it may be quite unlikely that certain speech would be useful to the listeners either for political purposes or for daily life purposes; this largely has to do with information that shows people in ridiculous, embarrassing, or demeaning contexts without revealing any useful new information about them. Everybody knows that I go to the bathroom; printing a picture of me on the toilet would embarrass me not because it reveals something new about me, but because it shows me in a pose that by cultural convention is seen as ridiculous or undignified.

This may explain cases such as *Daily Times Democrat v. Graham*,[180] where a newspaper was held liable for printing a picture of a woman whose dress was accidentally blown up over her waist, and it may partly explain why most people would gladly restrict the nonconsensual publication of photographs of people naked or having sex with their spouses.[181] These pictures aren't embarrassing because of the facts they reveal (except in rare cases where they show embarrassing deformities); everyone knows that we're all naked underneath our clothes, and that spouses generally have sex. Rather, they are embarrassing because these poses are conventionally seen as lacking in dignity. Whatever else sex may be, it isn't dignified, and while we may have little concern about our dignity while engaging in the act privately, this lack of concern may stem precisely from the fact that we know other people aren't watching.

But while there may be a narrow zone of fairly uncontroversially non-public-concern topics, the danger is that the vague, subjective "public concern," "newsworthiness," or "legitimate public interest" test will flow far beyond this zone; and as *Briscoe* and *Diaz*, among others, show, this danger has materialized. This risk may be enough to abandon the test altogether, and it is certainly enough to demand that the test be rephrased as something much clearer and narrower before it is accepted.

We can all think of examples of entertainment that has no connection to public issues, but *Winters v. New York* was right to conclude that entertain-

180. 162 So. 2d 474 (Ala. 1964).

181. *See, e.g.*, Melville B. Nimmer, *The Right to Speak from* Times *to* Time*: First Amendment Applied to Libel and Misapplied to Privacy*, 56 CAL. L. REV. 935, 961 (1968).

ment should be protected despite this, because "[t]he line between the informing and the entertaining is too elusive for the protection of [the] basic right [of free speech]."[182] If the word "fuck" were forcibly expurgated from public debate, discussion would likely not be substantially impoverished, but *Cohen v. California* was right to conclude that the word should be protected despite this, because otherwise "no readily ascertainable general principle [would] exist[] for stopping short of" far broader restrictions.[183] If vitriolic, relatively nonsubstantive parodies such as the one in *Hustler v. Falwell* were banned, "public discourse would probably suffer little or no harm," but the Court correctly refused to uphold such a ban, since it could find no "principled standard to separate" them from speech that had to be protected.[184] Likewise, the notion that otherwise protected speech should be restrictable when it doesn't relate to matters of public concern strikes me as so potentially broad and so vague that it deserves to be abandoned, even if it would yield the right results in a narrow subset of the cases in which it would be applied.[185]

C. *Doctrine*

That, then, is why I think the public concern test is theoretically unsound. The doctrinal discussion is easier: Though the Court has often said in dictum that political speech or public-issue speech is on the "highest rung" of constitutional protection,[186] it has never held that there's any general exception for speech on matters of "private concern." Political speech, scientific speech, art, entertainment, consumer product reviews, and speech on matters of private concern are thus all doctrinally entitled to the same level of high constitutional protection, restrictable only through laws that pass strict scrutiny.

The two situations where the Court has adopted a public concern / private concern distinction are narrow exceptions to this general principle. The first such exception, established in *Connick v. Myers,* is that the government acting as employer may freely restrict speech on matters of private concern by its employees.[187] The government's power as employer to fire its employees for what they say has always been far greater than its power to fine or imprison private citizens for what they say, and the *Connick* Court explic-

182. 333 U.S. 507, 510 (1948).

183. 403 U.S. 15, 25 (1971). *See also* note 11 *supra.*

184. 485 U.S. 46, 55 (1988).

185. Even Peter Edelman, a bitter critic of the Court's undermining of the tort in *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), acknowledges that "the private-fact disclosure cases create the slipperiest of slippery slopes." Edelman, *infra* note 268, at 1233.

186. Carey v. Brown, 447 U.S. 455, 467 (1980).

187. 461 U.S. 138 (1983).

itly stressed that private-concern speech remains protected against the government acting as sovereign.[188] The restriction on such speech by government employees was justified only by the special role of the government acting as employer, in which the government's interest in efficient day-to-day operation would make it infeasible to let people sue the government over every discharge that was based on any sort of speech.

The second exception, established in *Dun & Bradstreet v. Greenmoss Builders,* is that plaintiffs in libel cases involving false statements on matters of purely private concern may be awarded punitive and presumed damages without a showing of actual malice.[189] This, though, also came in a context where the government has special power to restrain speech: restrictions on false statements of fact.[190] Such statements, the Court has held, have "no constitutional value"[191]; any protection they get stems from the need to prevent the undue chilling of true statements, which are indeed constitutionally protected.[192] *Dun & Bradstreet* thus says little about the propriety of applying the "private concern" test to speech that, unlike false statements of fact, is presumptively constitutionally valuable.[193]

And *Dun & Bradstreet*'s reasoning confirms that the lower protection given to private-concern speech flows precisely from the speech being false and thus presumptively unprotected. The economic interests of the speaker and its audience, the Court argued, warrant no special protection when "*the speech is wholly false.*"[194] Likewise, the "chilling" effect on constitutionally protected true statements would be minimal because accurate credit reports are "hardy and unlikely to be deterred," are "more objectively verifiable,"

188. "We in no sense suggest that speech on private matters falls into one of the narrow and well-defined classes of expression which carries so little social value, such as obscenity, that the State can prohibit and punish such expression by all persons in its jurisdiction [and not just its own employees]." *Id.* at 147.

189. 472 U.S. 749 (1985).

190. *See* Estlund, *Speech on Matters of Public Concern, supra* note 159, at 12 ("The First Amendment was a late entrant into the fields of public employee speech and defamation law and has never held full sway within the two areas.").

191. 472 U.S. at 767 (White, J., concurring in the judgment). *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974).

192. *See Gertz,* 418 U.S. at 340-41.

193. *Cf., e.g.,* U.D. Registry, Inc. v. California, 40 Cal. Rptr. 2d 228, 232 (Ct. App. 1995) ("While the distinction [between private and public concern speech] may be significant in the area of defamation, it does not define the parameters of permissible regulation for truthful reporting."). A recent article argues that "[t]he first amendment right to publish personally-identified facts . . . is constrained . . . by a newsworthiness (or 'public concern') limitation," Cohen, *supra* note 10, at 1429 (citing Florida Star v. B.J.F., 491 U.S. 524 (1989)), but if that's a claim about existing doctrine, I believe it is mistaken. *Florida Star* did strike down an information privacy speech restriction based in part on the fact that the law barred speech on matters of public concern; but it explicitly refrained from deciding whether true statements on matters of private concern may be restricted. 491 U.S. at 532-33. As I argue in the text, the Court shouldn't carve out such an exception to free speech protection, but it certainly hasn't carved out such an exception so far.

194. *Dun & Bradstreet,* 472 U.S. at 762 (emphasis added).

and are in any case likely to have been heavily verified by successful credit agencies.[195] Neither verifiability nor the market pressure for accuracy is relevant outside the context of restrictions on false statements of fact.

D. *The Experience Under the Two "Public Concern" Doctrines*

In practice, neither of these doctrines has been a success story for the public concern test. As many critics have pointed out, the government employee private concern doctrine has proven both vague to the point of indeterminacy and extremely broad.[196] Much speech that would clearly fit within a normal reading of the words "public concern" has been found to be of purely private concern and therefore unprotected, with seemingly little justification other than the desire to make life easier for government employers confronted with troublemaking employees.

Connick itself found that speech among District Attorney's office employees about "the confidence and trust that [employees] possess in various supervisors, the level of office morale, and the need for a grievance committee" was "not of public concern," hardly a commonsense reading of the term "public concern." And in trying to flesh the test out further, the Court could only say that it was supposed to turn on the "content, form, and context" of the speech, an approach that virtually guarantees that the inquiry will be both unpredictable and little related to the phrase "public concern."[197]

Later cases have likewise found, for instance, that speech criticizing the way a dean runs a public university department,[198] alleging race discrimination by a public employer,[199] and criticizing the way the FBI decides whom to lay off[200] was not "of public concern," though other cases reached opposite results on seemingly similar facts.[201] Whether or not the government should have the power to dismiss employees for such speech, surely the government ought not have the power to censor such speech by citizens at large on the grounds that it's supposedly of insufficient "public concern."

Under *Dun & Bradstreet,* the concept of "speech of purely private concern" has ended up similarly vague, and has sometimes covered speech that clearly seems to be of public concern under any normal definition of the

---

195. *Id.*

196. *See, e.g.*, Stephen Allred, *From Connick to Confusion: The Struggle to Define Speech on Matters of Public Concern*, 64 IND. L.J. 43 (1988); Estlund, *Speech on Matters of Public Concern*, *supra* note 159, at 7 n.40, 34, 45.

197. 461 U.S. at 148. *Cf.* Estlund, *Speech on Matters of Public Concern*, *supra* note 159, at 34, which aptly describes the "content, form, and context" formulation as "strikingly vacuous."

198. Landrum v. Eastern Ky. Univ., 578 F. Supp. 241 (E.D. Ky. 1984).

199. Lipsey v. Chicago Cook County Criminal Justice Comm'n, 638 F. Supp. 837 (N.D. Ill. 1986).

200. Murray v. Gardner, 741 F.2d 434 (D.C. Cir. 1984).

201. *See generally* Allred, *supra* note 196, at 65-73.

term:[202] for instance, speech discussing the competence of psychologists to whom children are sent by government-run schools,[203] the business practices of car dealers,[204] and alleged misconduct by the owner of a gymnastics school.[205] Again, perhaps it's permissible to allow presumed and punitive damages for *false* statements on such topics, but surely it would be unconstitutional to restrict *true* statements on these matters on the grounds that they aren't of "public concern."

The experience of the public concern test in these two areas thus suggests that the theoretical criticisms of the public concern / private concern distinction are sound: There's a substantial practical risk of the courts finding too much speech to be of "private concern," and while some facially vague and broad tests have the merit of being tied to an existing body of clarifying and narrowing caselaw, that's hardly the case here. Maybe for want of anything better, the public / private concern distinction may remain sensible as to the genuinely hard and necessarily vague government employee speech cases, but its track record hardly seems to encourage expanding it elsewhere.

E. *Potential Consequences*

1. *Direct analogies.*

All this discussion is not just academic or just applicable to information privacy speech restrictions. The argument that certain speech should be more restrictable because it's not "political speech," not "high-value speech," or not of "legitimate public interest" is routinely marshaled in favor of a broad range of speech restraints.

The classic example is sexually themed speech. A recurring argument in favor of restrictions on such speech, from pornography to art to sexual humor, is that such speech has little to do with self-government, politics, or any of the important, legitimate topics of public debate.[206] What, the argument

---

202. *See* Robert E. Drechsel, *Defining "Public Concern" in Defamation Cases Since Dun & Bradstreet v. Greenmoss Builders*, 43 FED. COMM. L.J. 1, 17-18 (1990).

203. Saunders v. Van Pelt, 497 A.2d 1121 (Me. 1985).

204. Vern Sims Ford, Inc. v. Hagel, 713 P.2d 736 (Wash. Ct. App. 1986).

205. Ramirez v. Rogers, 540 A.2d 475 (Me. 1988).

206. *See, e.g.*, FCC v. Pacifica Found., 438 U.S. 726, 747 (1978) (plurality) (arguing that "patently offensive sexual and excretory language" may be restricted because it generally has lower "social value"); Young v. American Mini Theatres, Inc., 427 U.S. 50, 70 (1976) (plurality) ("[E]ven though we recognize that the First Amendment will not tolerate the total suppression of erotic materials that have some arguably artistic value, it is manifest that society's interest in protecting this type of expression is of a wholly different, and lesser, magnitude than the interest in untrammeled political debate . . . ."); Amicus Brief of Morality in Media, Inc. at 21, Reno v. ACLU, 521 U.S. 844 (1997) ("[T]he CDA provisions only affect speech which, in context, depicts or describes, in terms patently offensive, sexual or excretory activities or organs. Only a tiny fraction of communications

goes, is lost if such speech is restrained, especially if the restraint serves noble goals such as preserving morality, preventing antisocial attitudes, and shielding children against improper influences? Not political debate, not scientific discourse, just people saying and listening to things that they have no really good reason to say and listen to.

The more courts endorse some speech restrictions on the grounds that the First Amendment doesn't protect speech that's "not of legitimate public interest," the stronger this pro-restriction argument will be in other cases. Right now, the two areas where the courts have accepted a "public concern" test are at least cabinable as involving areas outside the core of First Amendment protection: restrictions imposed by the government acting as employer, where the government has always had a relatively free hand, and restrictions on false statements of fact, which already constitute a First Amendment exception. Analogies between, say, the Communications Decency Act and those restrictions can be rebutted by pointing out that the CDA involves the government acting as sovereign, restricting otherwise constitutionally protected speech.

Say, though, that courts accept a private concern justification for restrictions on speech that reveals personal information, which *are* restrictions on otherwise constitutionally protected speech imposed by the government acting as sovereign. Supporters of restrictions on sexually themed speech would then acquire several useful related arguments.

First, they would be able to argue that there is already a general "no public concern" exception to free speech protection.[207] Second, they could point to the information privacy speech restrictions as a specific precedent in favor of similar restrictions on sexually themed speech: Both, after all, involve restrictions on otherwise valuable speech imposed by the government acting as sovereign, and sexually themed speech, they'd argue, is no more important than are politicians' sexual identities or neighbors' criminal pasts. If courts accept the argument that personally identified data is unprotected because (1) it is not communicated "for its expressive content at all," (2) it is only "a tool for processing people, not a vehicle for injecting communication

necessary for government, research, education, politics, business and other matters of public concern, as well as for matters of private concern, may be indecent."); Cass R. Sunstein, *Words, Conduct, Caste,* 60 U. CHI. L. REV. 795, 797 (1993) ("Certain forms of pornography count as speech, but they are not plausibly intended or received as a contribution to political deliberation, and they fall within the low-value category.").

207. Even now, when the private/public concern distinction is limited to only two peripheral areas of free speech jurisprudence, Cindy Estlund warns that "the significance of the public concern test reaches well beyond the arenas of defamation and public employee speech; for what the Court did in *Connick* and *Dun & Bradstreet* could be done just as deftly in many other areas of First Amendment doctrine." Estlund, *Speech on Matters of Public Concern, supra* note 159, at 23. If Estlund is proven right, and the test works its way into decisions about what truthful statements newspapers may publish or database operators may communicate, then the risk of it being adopted in still other places will greatly increase.

into the 'marketplace of ideas,'"[208] and (3) "in the ways that matter, [it isn't] really 'speech' at all,"[209] some will quickly argue that sexually themed speech (1) is not communicated for its expressive content at all, (2) is only a tool for sexually arousing people, not a vehicle for injecting communication into the marketplace of ideas, and (3) in the ways that matter, isn't really speech at all.[210] What's more, information privacy speech restrictions are likely to prove quite popular; what better way to support your argument for restrictions on other "no public concern" speech than by analogizing not just to technical, little-known restrictions but to a widely liked and viscerally appealing one? Third, the precedential value of the government employee speech cases and libel cases would itself be strengthened. Right now these cases can be limited on the grounds that they don't involve the government as sovereign restricting otherwise valuable speech, but once those cases are accepted as an analogy for information privacy speech restrictions, such a limitation will be lost.

Those who want to protect sexually themed speech will try to distinguish it from speech that reveals private information. The definition of sexually themed speech, they'll argue, is either so vague or so broad that it includes matters that *are* of clearly legitimate public interest—discussions of sexually transmitted diseases, political statements about sexual matters that rely on graphic sexual imagery for their force, or moral or scientific statements about certain sexual subjects that are best made frankly and not through sanitized euphemism.[211] But the same, of course, is true of speech that communicates others' personal information, which often can be either of public interest or of daily life interest. If this argument is rejected for private information speech, it will also be easier to reject for sexually themed speech.

Likewise, opponents of restrictions on sexually themed speech will argue that the government has no business deciding which topics are "legitimate" and which aren't—that the First Amendment leaves this decision to speakers and listeners, not government officials. But again, if this argument is rejected for speech that reveals private information, and the government does get to decide that people really have no business talking about certain topics, the argument will also be much easier to reject for sexually themed speech.

Any new "no public concern" exception will help support other restrictions, too. Restrictions on profanity and on flag burning have been urged on

208. Cohen, *supra* note 10, at 1414.

209. *Id.* at 1418.

210. *See, e.g.*, Amicus Brief of Morality in Media, Inc. at 4, Reno v. ACLU, 521 U.S. 844 (1997) (arguing that the CDA is constitutional because the indecent speech that it banned is "no essential part of any exposition of ideas").

211. *See, e.g.*, Amicus Brief of the American Association of University Professors at 7, Reno v. ACLU, 521 U.S. 844 (1997) (arguing that discussion of certain subjects "necessarily entails frank and even graphic descriptions").

the grounds that the speech is not really necessary for the communication of important ideas;[212] campus speech codes have often been defended on the same grounds.[213] Though people have the right to express offensive or bigoted ideas, the argument goes, profanity, flag burning, and slurs don't really add anything much to such expression; the idea can still be expressed just as well without this valueless component. Bans on such speech, the argument might go, "would not damage the communication of a message," just as some argue that information privacy speech restrictions are constitutional because "[r]estraints on the circulation of personal information would not damage the communication of a message."[214] If courts accept the notion that publishing people's names in news stories can be restricted because the "need of the people to be informed of matters of general or public interest" could be "served as well without identifying" "the people concerned"[215] they will also be likely to uphold other government attempts to excise offensive and supposedly valueless components of other speech.[216]

Similarly, businesses criticized by disgruntled consumers have already argued that such consumer criticism doesn't relate to speech on matters of genuinely "public concern," and should therefore be restrictable even if it's true or if it's mere opinion.[217] Allowing tort liability under the disclosure tort for speech on supposedly "private matters" (such as a person's criminal history or failure to pay his debts[218]) would provide strong support for allowing tort liability under the intentional interference tort for speech on "private matters" (such as a business's unfair practices or breaches of warranty).

2. *Indirect influence.*

So far, I've discussed the purely doctrinal ways that accepting a "speech on matters of private concern" theory as to information privacy speech re-

212. *See, e.g.*, FCC v. Pacifica Found., 438 U.S. 726, 747 (1978) (plurality); Texas v. Johnson, 491 U.S. 397, 432 (1989) (Rehnquist, C.J., dissenting).

213. *See, e.g.*, Delgado, *infra* note 259.

214. Reidenberg, *supra* note 2, at 540.

215. Bloustein, *supra* note 179, at 93.

216. Consider also Sean Scott's proposal that "to properly balance freedom of the press against the right of privacy, every private fact disclosed in an otherwise truthful, newsworthy publication must have some substantial relevance to a matter of legitimate public interest." Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV. 683, 705 (1996). If the government may compel speakers to excise from their speech statements that lack "substantial relevance to a matter of legitimate public interest," then all sorts of bans on offensive forms of speaking would become permissible: Cohen's conviction for wearing a "Fuck the Draft" jacket could be upheld, for instance, on the theory that though his overall statement was on a matter of public concern, the word "Fuck" wasn't *substantially* relevant to expressing the "matter of legitimate public interest" at the core of Cohen's idea.

217. *See, e.g.*, Paradise Hills Assocs. v. Procel, 1 Cal. Rptr. 2d 514, 521 (Ct. App. 1991).

218. *See, e.g.*, Mason v. Williams Discount Ctr., Inc., 639 S.W.2d 836 (Mo. Ct. App. 1982).

strictions could support other proposed speech restrictions. Let me now suggest three other less direct but still significant ways in which this can happen.

First, "privacy" is a word with many meanings, and with such words both judges and laypeople often shift from one meaning to the other even in cases where the meanings have little in common. Consider how often privacy arguments commingle the *Griswold/Roe* constitutional right of decisional privacy, the Fourth Amendment right to privacy from physical government intrusion, and the four distinct privacy torts, even though these doctrines are at best distant cousins.[219] Or consider how often *Zacchini v. Scripps-Howard Broadcasting Co.* is cited for the proposition that a broad right of publicity is constitutional,[220] even though the case itself upheld only a narrow and unusual subset of the right of publicity—the right to block the rebroadcast of an entire act—on grounds that are specific to this narrow right and with the specific statement that it wasn't deciding the constitutionality of the broader right of publicity.[221] Our legal system (and perhaps human nature) operates by analogy, and analogies that rely on multiple meanings of the same word are unusually powerful.

Because of this, once restrictions on people's speech are accepted in the name of "privacy," people will likely use them to argue for other restrictions on "privacy" grounds, even when the matter involves a very different sort of "privacy." For instance, many people have already urged restrictions on sexually themed speech on the grounds that it invades people's "privacy" by being accessible in their homes (and thus in a way intruding on their seclusion), by being accessible to their children (and thus interfering with their "privacy" right to familial autonomy), or by lowering the moral tone of society in a way that affects people's most private relationships.[222]

---

219. *Cf. e.g.*, Edelman, *infra* note 268, at 1211 n.82 (suggesting, in my opinion without any support, that Justice Scalia's and Justice Kennedy's refusal to let privacy concerns trump free speech in *Florida Star v. B.J.F.* was tied to their hostility to the very different constitutional privacy right).

220. *See* note 79 *supra*; *see also* Diane Leenheer Zimmerman, *Who Put the Right in the Right of Publicity?*, 9 J. ART & ENT. LAW 35, 49-50 (1998) (discussing this phenomenon).

221. *See* note 78 *supra* and accompanying text.

222. *See, e.g.*, Bolger v. Youngs Drug Prods., 463 U.S. 60, 72 (1983) (considering and rejecting the federal government's argument that the mailing of contraceptive ads may be banned because it intrudes on recipients' privacy); FCC v. Pacifica Found., 438 U.S. 726, 748 (1978) (plurality opinion) ("Patently offensive, indecent material presented over the airwaves confronts the citizen, not only in public, but also in the privacy of the home, where the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder."); Amicus Brief of Morality in Media, Inc. at 11, Reno v. ACLU, 521 U.S. 844 (1997) ("Amicus would also argue that not just the well-being of children but also the privacy of the home needs protection from Internet indecency"); Sam Richards, *City of Livermore, Calif., Faces Internet Censorship Suit*, KNIGHT-RIDDER TRIB. BUSINESS NEWS, Dec. 24, 1998 (describing lawsuit claiming that libraries had a constitutional duty to block access by children to sexually themed material, on the grounds that such access violates "guarantees of a parent's fundamental rights to determine what their children learn"—this right is often described as a "privacy" right, *e.g.*, Bowers v. Hardwick, 478 U.S. 186, 204 (1986) (Black-

Second, a strong free speech principle necessarily requires the protection of speech that many sincerely believe is evil and dangerous. One way of mustering support for this principle, both among courts and among the public, is to stress that all sorts of groups are in this boat: If people are upset that the speech they hate is protected, they should take comfort in the fact that speech that they may like and that other people hate is protected, too.[223]

The converse of this, though, is that people's willingness to accept protection of the speech they hate decreases as they see new exceptions carved out for restrictions on other speech which they may see as much less harmful. We see this reaction already: Why should the harm that racist advocacy imposes on its victims remain unremedied, some supporters of campus speech codes ask, when harms to copyright owners, to libel victims, and the like have been found to justify punishment?[224] One article even makes the same argument in favor of information privacy speech restrictions themselves: "If the powerful may exert property rights or invoke contractual obligations to prevent or limit speech" (alluding to the existing free speech exceptions for contract law, trademark law, and contract law), "so too may others" asserting informational privacy rights.[225]

But the longer the list of permissible restrictions, the stronger these arguments for further restrictions will be. Imagine that the Court upholds in-

---

mun, J., dissenting)); Alexander Bickel, *On Pornography: Dissenting and Concurring Opinions*, 22 THE PUBLIC INTEREST, Winter 1971, at 25, 25-26 ("A man may be entitled to read an obscene book in his room, or expose himself indecently there. . . . We should protect his privacy. But if he demands a right to obtain the books and pictures he wants in the market, and to foregather in public places—discreet, if you will, but accessible to all—with others who share his tastes, then to grant him his right is to affect the world about the rest of us, and to impinge on other privacies. . . . [W]hat is commonly read and seen and heard and done intrudes upon us all, want it or not."), *quoted approvingly in* Paris Adult Theatre I v. Slaton, 413 U.S. 49, 59 (1973).

223. *See, e.g.*, the famous quote from Justice Black cited at note 294 *infra*.

224. Richard Delgado & Jean Stefancic, *Ten Arguments Against Hate-Speech Regulation: How Valid?*, 23 N. KY. L. REV. 475, 484 (1996) ("Powerful actors like government agencies, the writers' lobby, industries, and so on have always been successful at coining free speech 'exceptions' to suit their interest—copyright, false advertising, words of threat, defamation, libel, plagiarism, words of monopoly, and many others. But the strength of the interest behind these exceptions seems no less than that of a black undergraduate subjected to vicious abuse while walking late at night on campus."); Richard Delgado & David H. Yun, *Pressure Valves and Bloodied Chickens: An Analysis of Paternalistic Objections to Hate Speech Regulation*, 82 CAL. L. REV. 871, 892 (1994) ("Perhaps . . . in twenty or fifty years we will look upon hate speech rules with the same equanimity with which we now view defamation, forgery, obscenity, copyright, and dozens of other exceptions to the free speech principle, and wonder why in the late twentieth century we resisted them so strongly."); Martin E. Lee, *The Price We Pay: The Case Against Racist Speech, Hate Propaganda and Pornography*, NAT'L CATHOLIC REP., Oct. 4, 1996, at 17 (book review) ("Noting routine exceptions to free speech absolutism (copyright, trademark and such) that hew to business interests, the essays cite studies that document the heavy toll inflicted by the multibillion dollar porn industry, as it profits from a kind of hate speech that degrades women and children. . . . This book provides a sober rejoinder to cliche-ridden thinking by highlighting the profound power imbalance and social inequities that dim the luster of the First Amendment.").

225. Cohen, *supra* note 10, at 1421.

formation privacy speech restraints. Why should the harm to my child and my family stemming from the child's exposure to online indecency remain unprevented, some may then argue, when the indignity that someone feels from having his shopping habits communicated by one business to another justifies a speech restriction? Both, after all, involve nonpolitical speech. Neither involves threats of violence, or false statements of fact, or any other traditionally accepted reason why the speech should be treated differently. If your favorite restriction is accepted on "private concern" grounds, some will ask, why not mine? If some people may exert a growing list of rights to prevent or limit speech, after all, so too may others.

Finally, and relatedly, free speech is not always an intuitively appealing or intuitively delineated principle. Many people's commitment to protection of speech is neither ideologically very deep nor at the forefront of their thoughts. In this situation, the law as it is profoundly influences people's evaluation of the law as it should be (what some call "the normative power of the actual"[226])—just recall how often you've heard people argue "well of course this restriction should be permissible, look how many similar restrictions there are."[227] As more restrictions of a particular genre are in fact al-

---

226. *See* Morris R. Cohen, *The Basis of Contract*, 46 HARV. L. REV. 553, 582 (1933) (attributing the phrase to Georg Jellinek).

227. A recent defense of information privacy speech restrictions provides an excellent illustration of my concerns. "[W]e regulate the exchange of information as property all the time," the argument goes:

> [T]he law routinely allows private parties to invoke property ... rights to restrict others' speech. If collections of personally-identified data are like other sorts of regulated information, or if individuals have property or contractual interests that extend to (at least some) personally-identified information on an ongoing basis, the First Amendment landscape changes.... The law affords numerous instances of regulation of the exchange of information as property or product.

Cohen, *supra* note 10, at 1416. The argument goes on to give examples: "securities laws and regulations," "[l]aws prohibiting patent, copyright, and trademark infringement, and forbidding the misappropriation of trade secrets," and "federal computer crime laws," *id.* at 1416-17.

Note the structure of the argument: Certain kinds of speech restrictions, the argument says, are familiar, well-established, "routine," "numerous," happen "all the time." What's the big deal about another such restriction? The analogy between the supposed precedents and the proposed new restriction is not perfect; some of these restrictions—for instance, securities laws and federal computer crime laws—are justified for reasons quite unrelated to intellectual property: Securities laws are allowed because the government may restrict false or misleading commercial advertising. *See, e.g.*, Rubin v. Coors Brewing, 514 U.S. 476, 492 n.1 (1995) (Stevens, J., concurring in the judgment); Riley v. National Federation for the Blind, 487 U.S. 781, 796 n.9 (1988). The computer crime laws, as the argument itself acknowledges, Cohen, *supra* note 10, at 1417, are justified for reasons entirely unrelated to the communicative aspects of speech. Patent law generally doesn't restrict speech, outside a few highly unusual and controversial contexts. *See* Lemley & Volokh, *supra* note 119, at 232-37. Likewise, some of these laws, for instance the laws forbidding downstream communication of trade secrets by people who are under no contractual obligation to the trade secret owner, have never been validated by the Supreme Court. *See* text accompanying notes 86-96 *supra*. Still, though, the argument rests on the notion that the analogy is close enough that it should prevail. Given the speech restrictions we tolerate, we ought to tolerate this somewhat similar one, too.

lowed, many people will become more used to the notion that such restrictions are normatively proper, and will become more sympathetic to other restrictions of that genre. In Madison's words, once the power to enact certain restrictions "strengthen[s] itself by exercise, and entangle[s] the question in precedents," it becomes far more likely to generate other, still broader restrictions. This is why a "prudent jealousy" of government restraints on constitutional rights, even when the restraints are urged in a seemingly good cause, is indeed "the first duty of citizens."[228]

The law of course already allows quite a few speech restrictions, including restrictions justified on a "not of public concern" theory. But the Court has been careful to draw even those restrictions narrowly: The plurality opinions in *Young v. American Mini Theatres* and *FCC v. Pacifica Foundation,* for instance, upheld certain restraints on supposedly not very important speech such as pornography or profanity, but at the same time stressed that the restraints only regulated the time and place where the speech is communicated.[229] The restrictions on speech that reveals personal information

---

This is exactly the sort of argument that I fear will be used to urge still broader speech restraints if information privacy speech restrictions are upheld. "[W]e regulate the exchange of information as property all the time," the argument would go. "[T]he law routinely allows private parties to invoke property or contract rights to restrict others' speech. The law affords numerous instances of regulation of the exchange of information as property or product." The argument would then list the new, broadened list of intellectual property speech restrictions, which would for the first time include a Supreme-Court-sanctioned restraint on the communication of facts. And this list, the argument would contend, supports database protection legislation, a hot news misappropriation tort, a broadened right of publicity that would (for instance) block unauthorized biographies, or even an intellectual property right in the U.S. flag or in religious or cultural symbols. *See* notes 52-54 and 123-126 *supra*. Not perfect analogies, of course, but neither is the analogy between information privacy speech restrictions and computer crime laws, patent law, and regulations of securities offerings. If that analogy is good enough for courts, the hypothetical one I describe would be even stronger.

228. Madison, *supra* note 11.

229. Young v. American Mini Theatres, Inc., 427 U.S. 50, 71 (1976) (plurality opinion) ("what is ultimately at stake is nothing more than a limitation on the place where adult films may be exhibited"); FCC v. Pacifica Found., 438 U.S. 726, 750 (1978) (plurality opinion) (stressing "the narrowness of our holding," which applies only to broadcasting); *id.* at 760 (1978) (Powell, J., concurring in the judgment) (stressing that the ruling applies only to broadcasting, and "does not prevent respondent Pacifica Foundation from broadcasting the monologue during late evening hours when fewer children are likely to be in the audience"); *see also* Action for Children's Television v. FCC, 932 F.2d 1504 (D.C. Cir. 1991) (striking down a round-the-clock ban on broadcast indecency on the grounds that Pacifica allows only time restrictions on such broadcasts and not total bans). Moreover, recent cases seem to have in some measure undermined the precedential value of *Young* and *Pacifica. See, e.g.*, Reno v. ACLU, 521 U.S. 844, 861 (1997) (applying strict scrutiny, the test used to protect high-value speech, to strike down a restriction on the same sort of speech that *Pacifica* described as "low value," and distinguishing *Pacifica*); R.A.V. v. City of St. Paul, 505 U.S. 377, 390 n.6 (1992) (stressing that the *Young* and *Pacifica* pluralities "did not command a majority of the Court"); *cf.* Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141, 182 n.145 (arguing that *Reno*'s distinction of *Pacifica* is unsound, though ultimately concluding that *Pacifica* was mistaken).

would impose much broader bans than those approved in *Young* and *Pacifica*.

And more importantly, the precedential influence that I describe is never all or nothing. Arguing by analogy to one restriction is hard, both because that restriction looks like an unusual exception and because few proposed restrictions will be closely analogous to it. Arguing by analogy to two restrictions is easier, by analogy to several restrictions easier still. Political tacticians know this, which is why they are often willing to proceed step by step, building a body of political precedent that will make further steps easier and easier. Legal tacticians know this too; consider the NAACP's successful campaign to erode "separate but equal" one step at a time. Those who want to defend legal principles from erosion should also keep it in mind.

VI. COMPELLING INTEREST

The last argument for many proposed information privacy speech restrictions is that the government interest behind the restriction is just so great. Speech that reveals personal information about others, the argument goes, violates their basic human rights, strips them of their dignity, causes serious emotional distress, interferes with their relations with family, friends, acquaintances, and business associates, and puts them at risk of crime. Moreover, such speech itself undermines other rights of constitutional stature, such as the right to privacy or free speech itself. The government must be able to step in and prevent this, even at the cost of creating a new free speech exception.

A. *Countervailing Constitutional Rights*

Let me begin by discussing the "constitutional tension" argument, which comes in two flavors: (1) Because the Constitution has been interpreted as protecting privacy (possibly including information privacy[230]), attempts to restrict speech in the name of protecting information privacy involve a "tension" between two constitutional values.[231] (2) Information privacy speech restrictions "promote[] some of the same values protected by the First Amendment," because "[g]ranting people privacy, recognizing that despite their entering into the public debate on an issue . . . they remain a private

230. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977) (stating that "in some circumstances that duty [of government nondisclosure] arguably has its roots in the Constitution").

231. *See also* Melvin v. Reid, 112 Cal. App. 285, 291 (1931) (recognizing the disclosure tort in part on the theory that the California Constitution protects "[t]he right to pursue and obtain happiness," which is jeopardized even by true revelations that "unwarranted[ly] attack . . . one's liberty, property, and reputation," but not explicitly discussing the free speech question).

person to some degree, encourages people to come forward and engage in the debate."[232]

I have elsewhere argued at length against this sort of analysis,[233] but for now let me make two observations about it. First, the speech vs. privacy and speech vs. speech tensions are not tensions between constitutional rights on both sides. The Constitution presumptively prohibits government restrictions on speech and perhaps some government revelation of personal information, but it says nothing about interference with speech or revelation of personal information by nongovernmental speakers.[234]

If, for instance, a private group organizes a boycott of a newspaper to pressure it into dropping a columnist whose work the group finds offensive,[235] the group is not thereby violating the columnist's First Amendment rights; he has a constitutional right to speak free from government restraint, but not free from private censure or private pressure. Likewise, information privacy speech restrictions involve a tension between a *constitutionally secured* right to speak free of government restriction and a proposed *statutory or common-law* right to speak free of private revelation of private information. The fact that the proposed statutory or common-law right is in one way analogous to a constitutional right does not give it constitutional stature.

Second, as the boycott example shows, changing First Amendment doctrine to let free speech rights be trumped by other "constitutional values" derived by analogy from constitutional rights would permit a broad range of

---

232. Scott, *supra* note 216, at 687, 710. *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1701-02, 1651 (1999) (arguing that information privacy speech restrictions are needed to "promot[e] democratic deliberation . . . in cyberspace," because "[i]n the absence of strong rules for information privacy, Americans will hesitate to engage in cyberspace activities—including those that are most likely to promote democratic self-rule"); Schwartz, *supra* note *, at 1563-64.

233. Eugene Volokh, *Freedom of Speech and the Constitutional Tension Method*, 3 U. CHI. L. SCH. ROUNDTABLE 223 (1996).

234. Some state constitutional provisions might bar "invasions of privacy" by private actors, *see, e.g.*, Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 672 (Cal. 1994), but this can't justify a violation of federal free speech rights. *See* Widmar v. Vincent, 454 U.S. 263, 276-77 (1981).

235. *See, e.g.*, Jill Stewart, *Free This Man; Can Black Conservatives Speak Their Minds in America? Ask KABC Talk-Show Host Larry Elder, the Target of a Black Nationalist Group in L.A.*, NEW TIMES (L.A.), July 3, 1997 (describing boycott of sponsors of black conservative talk show host Larry Elder's radio show, aimed at getting the radio station to take him off the air); James Warren, *Andy Rooney Suspended, But Denies Racist Comment*, CHI. TRIB., Feb. 9, 1990, § 1, at 3 (describing public pressure that caused CBS to suspend *60 Minutes* commentator Andy Rooney for allegedly making a racist comment); Jerry Berger, *Kennedy Decries Reagan Civil Rights Policies*, United Press Int'l, Jan. 18, 1988, *available in* LEXIS, News Library, UPI File (describing public pressure that caused CBS to fire Jimmy "The Greek" Snyder on similar grounds); Youth for Justice, "Tonight's Menu" (flyer listing various San Francisco business owners and others who contributed to the California Civil Rights Initiative, saying that "[t]hey've left a bad taste in our mouths with their dirty donations to CCRI," and implicitly but pretty clearly calling for a boycott of at least one of the businesses, a restaurant) (on file with author).

speech restrictions. Lots of speech has the effect, and often the purpose, of discouraging people from exercising their speech rights in certain ways. Political bullies try to silence their opponents not only by revealing embarrassing private information about them, but also by calling them nasty (but nonlibelous) names,[236] citing their interracial marriages as evidence that they are traitors to their race,[237] attacking them with bitter and unfair parodies,[238] or saying things aimed at undermining their business affairs.[239] Depending on the era, the risk of having your arguments called "Communist," "un-American," "racist," or "sexist" (even if your arguments really don't fall into those categories)[240] has discouraged many people from expressing viewpoints that might draw such rhetoric—and I suspect that the rhetoric was often used precisely to deter people from expressing certain viewpoints. Who among us hasn't at times decided to stay quiet in order to avoid having to deal with our opponents' vituperation?

---

236. *See, e.g.*, John L. Mitchell, *Larry Knows Best*, L.A. TIMES, May 31, 1998, Magazine sec., at 12 ("Out of the black community came anonymous fliers accusing [conservative black talk show host Larry] Elder of hate speech, describing him as a 'White Man's Poster Boy' and a 'boot-licking Uncle Tom.'"); Rick Pearson & Graeme Zielinski, *Senator Apologizes for Epithet*, CHI. TRIB., Sept. 8, 1998, at 1 (quoting Sen. Carol Moseley-Braun's response to columnist George Will's criticism of her: "'I think because he could not say 'nigger,' he said the word 'corrupt,'" Moseley-Braun said, although the word 'corrupt' did not appear in the conservative commentator's column. 'George Will can just take his hood and go back to wherever he came from,' she added, apparently alluding to hoods worn by members of the Ku Klux Klan."); *The News No Longer With Keith*, THE HOTLINE, Dec. 3, 1998 (People section) (quoting MSNBC anchor Keith Olbermann as saying, while criticizing Ken Starr's investigation of Bill Clinton, "It finally dawned on me that the person Ken Starr has reminded me of, facially, all this time was Heinrich Himmler, including the glasses").

237. *See, e.g.*, Amy Wallace, *He's Either Mr. Right or Mr. Wrong*, L.A. TIMES, Mar. 31, 1996, at 12 ("State Sen. Diane Watson of Los Angeles accused [Ward Connerly, leader of the California anti-race-preference campaign] of selling out his own people. 'He probably feels this makes him more white than black, and that's what he really wanted to be,' she said, adding, 'He married a white woman.'").

238. *See, e.g.*, Hustler Magazine v. Falwell, 485 U.S. 46 (1988).

239. *Cf., e.g.*, Jill Hodges, *Planned Parenthood List of Donors in Rivals' Hands*, MINN. STAR TRIB., Mar. 19, 1992, at 1A (describing plans of anti-abortion activists to boycott and picket corporations that contribute to Planned Parenthood); Charles V. Zehren, *Caught in Abortion Crossfire; Both Sides Pressure Firms*, NEWSDAY, Aug. 13, 1989, at 6 (describing National Organization for Women's boycott of Domino's Pizza, whose chief executive was giving money to anti-abortion groups); *supra* note 235.

240. Calling a person a "Communist" or "racist" might be seen as a legally actionable false statement of fact, since it may imply that the person has certain specific views or has engaged in certain specific acts, though even that isn't certain. *See* Stevens v. Tillman, 855 F.2d 394, 402 (7th Cir. 1988) (Easterbrook, J.) ("Accusations of 'racism' no longer are 'obviously and naturally harmful.' The word has been watered down by overuse, becoming common coin in political discourse.... In daily life 'racist' is hurled about so indiscriminately that it is no more than a verbal slap in the face.... It is not actionable unless it implies the existence of undisclosed, defamatory facts."). In any event, though, calling an argument or a viewpoint "Communist" or "racist" does not contain such a factual implication, and is thus a statement of opinion and not punishable by libel law.

Consider a telling example from an article arguing that information privacy speech restrictions serve free speech values: "[S]tudies indicate that the threat of continued exposure to adverse public opinion curtails an individual's willingness not only to voice dissenting or nonconformist opinions but also curtails the willingness to entertain such positions privately."[241] Exactly right—the threat of *adverse public opinion,* whether it flows from the revelation of embarrassing personal information about the speaker, demagoguery about the supposed heinousness of his views, pure insults, or for that matter reasoned counterargument, does deter speech. The logic of the argument I quoted, if accepted, would thus justify restriction on all these kinds of speech.[242] And yet our right to use speech to pressure others into not speaking is a fundamental aspect of the First Amendment; recall that a recurring (and correct) argument of those who fight against advocacy of evil ideas—even advocacy that is concededly constitutionally protected against government suppression—is that such speech should be deterred by social ostracism and condemnation.

Likewise, accepting the other constitutional tension argument, which urges that speech be restricted when it undermines the unwritten constitutional "value" of privacy, would provide strong support for restrictions on speech that vehemently criticizes a religion and thereby discourages people

---

241. Scott, *supra* note 216, at 717.

242. The article making this argument doesn't confront this implication of its proposal. It does try to distinguish its proposed privacy-based speech restrictions from libel law, but this attempt only shows that such distinctions are very hard to draw:

> The value protected by defamation is an individual's interest in her reputation. The First Amendment values protected [by constitutional restraints on libel law] can include the search for truth, self-governance, and any number of other values. In essence, individual rights are being weighed against societal rights. With privacy, on the other hand, the interest protected is not merely the interest in one's dignity, but rather the interests in the search for truth, autonomy and self-governance. Because the values being served by the plaintiff's privacy action are First Amendment values rather than simply human dignity, it is inappropriate to adopt the defamation model.

Scott, *supra* note 216, at 725-26. Of course one standard argument for broad libel law is precisely that falsehoods interfere with the public's "search for truth" and well-informed "self-governance," and with the victim's "autonomy" (which the article defines as "[s]elf-realization and [i]ndividuality," Scott, *supra* note 216, at 717). *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 392, 400 (1974) (White, J., dissenting) (arguing that libel "may frustrate th[e] search [for truth]" and contribute to "assaults on individuality and personal dignity"). In fact, Justice White, the Court's most vocal exponent of decreasing constitutional protections against libel actions, has explicitly argued that First Amendment protections in libel cases should be reduced because the risk of defamation may deter people from entering public life. *See, e.g., id.* at 400 ("It is not at all inconceivable that virtually unrestrained defamatory remarks about private citizens will discourage them from speaking out and concerning themselves with social problems. This would turn the First Amendment on its head."). Elsewhere the article I criticize repeats a similar argument. *See* Scott, *supra* note 216, at 712-13.

The article's proposed distinction is thus no distinction at all—just another piece of evidence that speech restrictions created in the name of information privacy are far harder to distinguish from other speech restrictions than some might think.

from publicly adhering to it (and thus supposedly undermines the explicitly constitutionally described values of religious freedom),[243] speech that urges people to treat others unequally (and thus undermines equality), speech that tries to pressure people into not exercising their property or contractual rights (and thus undermines private property rights or the obligation of contracts), and so on.[244] A rule that constitutional rights to protection from the government may be turned into justification for government restrictions on speech by private actors would have a broad effect indeed.

B. *Dignity, Emotional Distress, and Civil Rights*

Other arguments for information privacy speech restrictions claim that the speech injures people's dignity or emotionally distresses them. This injury is sometimes also characterized as an interference with people's basic "civil right" not to have others know or say certain things about them.[245]

Some of the more extreme claims put this in rather extravagant terms: "[A] rampant press feeding on the stuff of private life would destroy individual dignity and integrity and emasculate individual freedom and independence."[246] "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different . . . . Such a being, although sentient, is fungible: he is not an individual."[247] Without privacy, "intimate relationships simply could not exist."[248] "Privacy is an essential part of the complex social practice by means of which the social group recognizes—and communicates to the individual—that his existence is his own. And this is a precondition of personhood."[249]

---

243. *Cf., e.g.*, Kunz v. New York, 340 U.S. 290, 295, 302 (1951) (Jackson, J., dissenting).

244. *See generally* Volokh, *supra* note 232, at 231-34, 237-38.

245. *See, e.g.*, Directive 95/46/EC, art. 1(1) 1995 O.J. (L.281) 31 (describing protection of informational privacy as a matter of "the fundamental rights and freedoms" "of natural persons"); Cohen, *supra* note 10, at 1423-24 (seemingly endorsing this view); *Talk of the Nation: Online Privacy* (NPR radio broadcast, June 30, 1998) (quoting Todd Lappin, senior associate editor of *Wired* magazine) ("[I]t's really the job of all of us to get a consensus in Congress that'll give us basic legal rights so we have some control over our names and over our personal information. This is a civil rights and a human rights struggle . . . .").

246. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962 (1964), *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 156, 163 (Ferdinand D. Schoeman ed., 1984) (characterizing Warren & Brandeis as implicitly taking this view, and ultimately endorsing the view himself).

247. *Id.* at 1003.

248. Robert S. Gerstein, *Intimacy and Privacy*, 89 ETHICS 76, 76 (1978).

249. Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 39 (1976).

It's not entirely clear what exactly these claims mean. If the assertion is simply that *complete* lack of privacy—a situation where people are indeed compelled to live "every minute" among others and where their "every . . . thought" is indeed subject to public scrutiny—would dramatically affect freedom and intimacy, that might be true. It would be grim indeed to live in a hypothetical environment where there is no private property, where the government constantly listens to and watches every conversation, where some thought-reading device reaches into people's heads (the only way in which literally "every . . . thought" would be subject to scrutiny), and where there are no market pressures, contracts, or social conventions that prevent monitoring or revelation of private information.

But of course this grim vision tells us little about any supposed need for extracontractual prohibitions on nongovernmental speech that reveals personal information. Even if all such speech restrictions were unconstitutional, we'd still have a world where much of our privacy can be protected by legal rules that restrain private trespass, wiretapping, and electronic eavesdropping; by constitutional restraints on government searches; by statutory restraints on government collection and revelation of personal information; by contractual obligations on the part of people to whom we must reveal data; by market pressure on many businesses not to reveal data about their customers;[250] by technological self-protection that can hide our identity in many online transactions;[251] and by social norms. Some might still think that this world permits undue intrusions on privacy, but it hardly seems to risk the actual destruction of dignity, integrity, freedom, and independence, or the impossibility (not just difficulty, but impossibility) of intimacy and even personhood.

Claims about what would happen if privacy were totally destroyed tell us nothing about which particular privacy rules (and especially which restrictions on others' constitutional rights) are indispensable. To give an analogy, one might plausibly argue that a society where "every minute of [one's] life"—at home, in public, reading a newspaper, or watching television—one is constantly confronted with nongovernmental proselytizing of a particular religion and with warnings of hellfire and damnation if one doesn't conform would rob people of dignity, integrity, freedom, individuality, and intimacy.

250. *See, e.g.*, Justin Matlick, *Governing Internet Privacy: A Free-Market Primer* (Pacific Research Institute, July 1999), (visited March 3, 2000) <http://www.pacificresearch.org>.

251. *See, e.g.*, Kang, *supra* note 28, at 1241-45; Gindin, *supra* note 1, at 1176-79; Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO POLICY ANALYSIS NO. 295 (Jan. 22, 1998) <http://www.cato.org/pubs/pas/pa-295.html>, at text accompanying nn. 74 & 75.

But such an argument provides no support for the government banning nongovernmental proselytizing in the society we have today.[252]

On the other hand, if the claim is that the ability of private parties to communicate personal information about others *by itself* "destroy[s] individual dignity and integrity and emasculate[s] individual freedom and independence," "deprive[s people] of [their] individuality," makes it impossible for "intimate relationships [to] exist," or denies that a person's "existence is his own," such a claim is simply false. Today, private parties do have very broad rights to communicate personal information about us, but because of the other protections described above, our dignity, freedom, individuality, and capacity for intimacy still seem largely intact. I suppose it's theoretically conceivable that at some unknown future time information technology might get so powerful that these values will indeed be threatened with "destruction" by such speech; but free speech—whether it's speech that reveals personal information, speech that communicates socially harmful ideas, or speech that allegedly coarsens public discourse[253]—ought not be restricted today merely on the grounds that some decades hence such speech might possibly "destroy individual dignity."[254]

Once the hyperbole is set aside, there remain some more modest claims. Speech that reveals private information about people may not destroy individuality or dignity, but some argue that it does diminish their dignity,[255] that it can severely distress them, that it fails to properly respect them,[256] and that it interferes with a basic civil right not to have people communicate such information.

---

252. *Cf.* Cantwell v. Connecticut, 310 U.S. 296, 303-04, 309-10 (1940) (holding that such proselytizing, even when it vitriolically condemns other religions, is constitutionally protected); Kunz v. New York, 340 U.S. 290, 294 (1951) (same).

253. *Cf., e.g.*, Kingsley Int'l Pictures Corp. v. Regents, 360 U.S. 684, 688-89 (1959) (holding that advocacy of adultery is constitutionally protected); Brandenburg v. Ohio, 395 U.S. 444 (1969) (holding that even advocacy of violence is constitutionally protected); Cohen v. California, 403 U.S. 15 (1971) (holding that profanity is constitutionally protected).

254. Some might possibly argue—similarly to the way that I argue about free speech—that while nongovernmental revelation of personal information does not by itself "destroy individual dignity," it can set precedents that will over time lead to greater and greater trespasses on other kinds of privacy, and thus eventually destroy dignity. But while this is a possible argument, I have not seen it made in any detail, and my tentative reaction to it is skeptical: I just don't see how people's ability to freely speak about others would lead to, for instance, more unreasonable searches and seizures, more government intrusions on reproductive decisions, or more private wiretaps or trespasses. Perhaps there is a persuasive, concrete argument explaining the mechanisms through which this long-term destruction of individual dignity might take place; but I haven't seen it.

255. *Cf.* Melville G. Nimmer, *The Right to Speak from* Times *to* Time*: First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CAL. L. REV. 935, 959 (1968) (arguing that public disclosure of private information "degrad[es] a person by laying his life open to public view").

256. *Cf.* Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 223, 228-29 (Ferdinand D. Schoeman ed. 1984).

But is it constitutional for the government to suppress certain kinds of speech in order to protect dignity, prevent disrespectful behavior, prevent emotional distress, or to protect a supposed civil right not to be talked about? Under current constitutional doctrine, the answer seems to be no. Though the Supreme Court has sometimes left open the door to the possibility of restricting truthful speech simply on those grounds,[257] the general trend of the cases cuts against this: Even offensive, outrageous, disrespectful, and dignity-assaulting speech is constitutionally protected.[258]

And there is good reason for this approach. All of us can imagine some speech that is so offensive and at the same time so valueless that we would feel no loss if it were restricted, but the trouble is that each of us has a somewhat different vision of which speech should qualify. The more courts conclude that avoidance of disrespect or emotional distress is a "compelling interest" that justifies restricting the speech we find worthless, the more likely they will be to accept the same arguments for restricting the speech we value.

Just consider how many proposed new exceptions have been urged on the grounds that they protect "basic human rights" or people's "dignity." Proposed bans on "hate speech," on university campuses or elsewhere, have been defended on exactly these grounds, and their supporters have likewise argued that such speech causes serious emotional distress, interferes with the target groups' social and business opportunities, and lacks constitutional value to boot.[259] The same has been said for sexually themed speech, which many people argue strips all women of their dignity, interferes with the personal and business relationships of women who have to deal with men who watch such speech, and is irrelevant to matters of public concern.[260]

---

257. *See, e.g.*, Florida Star v. B.J.F., 491 U.S. 524, 532-33 (1989) (leaving open the possibility that speech that reveals highly embarrassing information might be punished if it does not involve matters of private concern); Hustler Magazine v. Falwell, 485 U.S. 46, 50 (1988) (holding that otherwise protected speech about a public figure may not be restricted on the grounds that it is outrageous and inflicts severe emotional distress, but not discussing speech about private figures); Garrison v. Louisiana, 379 U.S. 64, 72, 73 n.8 (1964) (holding that truth must be an absolute defense as to matters of public concern, but leaving open the possibility that it may not be a defense to charges that a statement on matters of private concern has injured someone's reputation).

258. *See, e.g.*, Cohen v. California, 403 U.S. 15 (1971) (public profanity); Texas v. Johnson, 491 U.S. 397 (1989) (flag burning); Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (scurrilous, personal attack in print); Brandenburg v. Ohio, 395 U.S. 444 (1969) (racist advocacy); Collin v. Smith, 578 F.2d 1197 (7th Cir. 1978) (Nazi parade in a part of town where many Holocaust survivors lived); Kunz v. New York, 340 U.S. 290 (1951) (vitriolic attacks on Catholicism and Judaism); Cantwell v. Connecticut, 310 U.S. 296 (1940) (vitriolic attack on Catholicism).

259. *See generally* Mari J. Matsuda, *Public Response to Racist Speech: Considering the Victim's Story*, *in* WORDS THAT WOUND: CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT 17 (Mari Matsuda et al. eds., 1993); Charles R. Lawrence III, *If He Hollers Let Him Go: Regulating Racist Speech on Campus*, *in id.* at 53; Richard Delgado, *Campus Antiracism Rules: Constitutional Narratives in Collision*, 85 NW. U. L. REV. 343 (1991).

260. *See, e.g.*, CATHERINE A. MACKINNON, ONLY WORDS (1993).

Jerry Falwell quite plausibly argued that Hustler's criticisms of him were extremely undignified, disrespectful, and distressing, and interfered with a legally recognized right to freedom from intentional infliction of severe emotional distress.[261] Proposed flag burning bans are defended on the grounds that such speech insults the dignity of veterans and of all Americans, is unnecessarily disrespectful, lacks substantial constitutional value, and inflicts severe emotional distress on those whose relatives died defending the nation for which the flag stands. Parents claim a civil right to not have their kids exposed to certain kinds of speech.[262]

If the government can declare it to be my "civil right" to prohibit others from saying the truth about me behind my back, then the arguments for these proposed restrictions and for many others would be considerably strengthened. The government could similarly declare it a civil right to have others not say insulting things about me (and my kind) in print or in broadcasts, where I may directly see or hear such speech; other countries have indeed done this. Similarly, say that *true* statements—statements about past crimes, current sexual orientation, credit history, and the like—can be restricted because of the danger that they will change people's attitudes about their subject. Why wouldn't sociological or political claims that the government considers false or misleading (group libel or seditious libel)[263] or statements of opinion (general bigoted or antigovernment advocacy) be likewise restrictable, on the grounds that they may change people's attitudes about a group, and that there's a "compelling governmental interest" in preventing such changed attitudes?

The same applies to sexually themed speech. Many people are offended by the very knowledge that men are reading and watching things that lead them to see women as sexual objects.[264] Many women rightly suspect that many men think of them in crude sexual terms, and perhaps may make sexually themed remarks about them behind their backs (which some see as an "invasion of privacy"). It's plausible that much sexually themed speech fosters such attitudes, and that sexually themed speech may influence its consumers' personal and business relationships with women. If the government has a compelling interest in preventing people from thinking highly offensive thoughts and saying highly offensive things about us behind our

261. Hustler Magazine v. Falwell, 485 U.S. 46 (1988).

262. *See, e.g.*, Richards, *supra* note 222.

263. *Cf., e.g.*, United States v. Cooper, 25 F. Cas. 631, 639 (C.C.D. Pa. 1800).

264. *See, e.g.*, Johnson v. County of Los Angeles Fire Dep't, 865 F. Supp. 1430, 1440 (C.D. Cal. 1994) (involving claim that even "quiet reading" of sexually themed magazines by firefighters should be banned because women coworkers were "offended . . . by the knowledge that men who read Playboy might entertain degrading thoughts about their coworkers").

backs in the information privacy context, why not in the sexually themed speech context?[265]

Proponents of information privacy speech restrictions might argue that such restrictions are different because speech that reveals private information about someone is of no legitimate public concern, or is not necessary to public debate. But many equally think that there's no legitimate reason for people to spread harmful opinions (and misleading sociological claims) about groups, to burn flags, to gratuitously insult public figures, or to display nude pictures to each other. Likewise, many argue that even if racist opinions are a legitimate subject of public debate, personal insults, racial slurs, profanities, sexually themed art, and explicit discussion of sexual subjects are not necessary to such debate, since it's possible to express one's views without such speech.

On the other side of the comparison, as Part V argued, a good deal of speech that reveals information about people, including speech that some describe as being of merely "private concern," is actually of eminently legitimate interest. Some of it is directly relevant to the formation of general social and political opinions; most of it is of interest to people deciding how to behave in their daily lives, whether daily business or daily personal lives—whom to approach to do business, whom to trust with their money, and the like. True, this speech isn't a candidates' debate, or an editorial regarding a ballot measure; allowing restrictions on this speech will only minimally jeopardize such intensely political advocacy. But the speech I describe is at least as relevant to people's lives as is much speech that is today constitutionally protected, be it art, product reviews, or humor; restricting it on "compelling interest" grounds will indeed set a precedent for restricting those other kinds of speech, too.

Beyond the purely legal precedent, though, I am especially worried about the normative power[266] of the notion that the government has a compelling

265. My concerns apply equally to proposals that frankly "prioritiz[e] privacy over speech." Joseph Elford, *Trafficking in Stolen Information: A "Hierarchy of Rights" Approach to the Private Facts Tort*, 105 YALE L.J. 727, 745 (1995); *see also* Thomas I. Emerson, *The Right of Privacy and Freedom of the Press*, 14 HARV. C.R.-C.L. L. REV. 329, 341 (1979). The more rights are prioritized over the constitutionally secured right to free speech, the likelier it is that courts will hold that other rights, new and old—freedom from intentional interference with emotional distress, freedom from interference with business relationships, freedom from speech that undermines equality, and the like—similarly trump free speech.

This is especially so when the reasons for treating privacy as superior to free speech are so generalizable. Consider the Elford article's argument that "speech has a greater propensity than privacy to cause individual harm" and that "[u]nlike the right to speech, which serves both individual and social interests, the benefits of privacy are entirely individual" and therefore more worthy, 105 YALE L.J. at 745-46. This argument could equally be made to justify the constitutional free speech right being trumped by any of the statutory or common-law rights I mention earlier in this footnote. The Emerson argument suffers from the same problem.

266. *See* text accompanying note 215 *supra*.

interest in creating "codes of fair information practices" restricting true statements made by nongovernmental speakers. The protection of free speech generally rests on an assumption that it's not for the government to decide which speech is "fair" and which isn't; the unfairnesses, excesses, and bad taste of speakers are something that current First Amendment principles generally require us to tolerate. Once people grow to accept and even like government restrictions on one kind of supposedly "unfair" communication of facts, it may become much easier for people to accept "codes of fair reporting,"[267] "codes of fair debate," "codes of fair filmmaking," "codes of fair political criticism," and the like.

It is conceivable that as to some kinds of speech, for instance the revelation of the names of rape victims or the unauthorized distribution of pictures of a person naked or having sex, courts will find that the speech is so valueless and so distressing that there is indeed a compelling interest in restricting it.[268] Though I empathize with the reasons for such restrictions, I reluctantly oppose them, precisely because of the dangers discussed in Part V and earlier in this section—"lack of legitimate public concern" and "severe emotional distress," while intuitively appealing standards, are so vague and potentially so broad that accepting them may jeopardize a good deal of speech that ought to be protected.[269]

But while these narrow restrictions would merely increase the risk that more speech might be restricted in the future, other proposed restrictions

---

267. *See supra* note 12.

268. Actually, the names of rape victims can often be quite relevant to discussions of public affairs. Even Peter Edelman, a strong supporter of allowing the media to be sued for revealing rape victims' names, lists a variety of cases where the names may be revealed:

> The speech interest is stronger when a question exists about the legitimacy of the rape complaint or whether the right person has been accused. An article that examines patterns in the attitudes of police and prosecutors concerning rape might capture reader attention more effectively if it names the actual rape victims whose cases the article addresses. Likewise, if numerous rapes occurred and aroused suspicion that the authorities were attempting to conceal their inability to make arrests, it might be important to the political process to state the names of the victims.

Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195, 1210-11 (1990). Given this long, diverse, and doubtless expandable catalog of cases where the name is newsworthy, it becomes hard to see how a clear, objective line can be drawn between "newsworthy" naming of the victim and "unnewsworthy" naming. Perhaps this should cut in favor of a per se rule barring the publication of rape victims' names, or perhaps we can tolerate a vague rule with the expectation (and perhaps desire) that newspapers will be chilled from publishing the victim's name even when this information would be newsworthy. But it can't be denied that either kind of rule will indeed suppress speech that's substantially related to matters of serious public concern.

269. One could make the same criticisms of the obscenity exception, and I agree with these criticisms. Fortunately, perhaps owing to the relative liberality of public and judicial mores since the 1970s (at least compared to the 1950s and earlier), the obscenity exception has in practice proven quite narrow; but I remain concerned about what would happen if judicial and social attitudes become more hostile to sexually themed expression. The fact that the Court has gone in this perilous direction before doesn't mean that we should encourage the Court to do so again.

cheerfully embrace this possibility. Broad readings of the disclosure tort would, as Part V argues, restrict speech about elected officials that many voters would (rightly or wrongly) find quite relevant, or restrict speech about people's past crimes, which many of the people's neighbors may find important.

Likewise, many of the proposals to restrict communication of consumer transactional data would apply far beyond a narrow core of highly private information, and would cover all transactional information, such as the car, house, food, or clothes one buys. I don't deny that many people may find such speech vaguely ominous and would rather that it not take place, and I acknowledge that some people get extremely upset about it. But knowing that some business somewhere knows what car you drive[270] is just not in the same league as, say, knowing that all your neighbors (and thousands of strangers) have heard that you were raped. If such relatively modest offense or annoyance is enough to justify speech restrictions, then the compelling interest bar has fallen quite low. And watering down the threshold for when an interest becomes "compelling" will of course have an impact far beyond information privacy speech restrictions.

Finally, on the purely doctrinal level, *Florida Star v. B.J.F.* made clear that information privacy speech restrictions are unconstitutional if they are underinclusive with respect to the interest in information privacy.[271] One of the reasons *Florida Star* gave for striking down the statutory ban on publishing the names of rape victims is that such a ban applied only to the media and not to the victim's acquaintances or neighbors. "[T]he communication of such information to persons who live near, or work with, the victim may have consequences as devastating as the exposure of her name to large numbers of strangers," the Court pointed out; and this "facial underinclusiveness ... raises serious doubts about whether Florida is, in fact, serving, with this statute, the significant interests which appellee invokes in support of affirmance."[272] This argument casts into doubt most states' disclosure torts, which also apply only to broad dissemination and not communication to a small group of acquaintances,[273] as well as bans on merchants (and not others) communicating clients' personal data.

---

270. *Cf., e.g.*, Gindin, *supra* note 1, at 1157.

271. *See* Eugene Volokh, *Freedom of Speech, Permissible Tailoring, and Transcending Strict Scrutiny*, 144 U. PA. L. REV. 2417, 2420 (1996) (discussing the underinclusiveness inquiry in detail).

272. Florida Star v. B.J.F., 491 U.S. 524, 540 (1989); *see also id.* at 542 (Scalia, J., concurring) (relying primarily on this point, and concluding that "This law has every appearance of a prohibition that society is prepared to impose upon the press but not upon itself. Such a prohibition does not protect an interest 'of the highest order.'").

273. *See* 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.9[C](1), at 5-100 (1999).

C. *Keeping the Internet Attractive to Consumers*

Some have argued that privacy restrictions are needed to keep Internet access attractive to consumers: Consumers are so concerned that online sites will collect and reveal information about them, the argument goes, that they are being deterred from engaging in e-commerce, and thus e-commerce in particular and the economy in general is suffering.[274]

It seems to me, though, that fostering economic growth and increasing Internet use, while laudable goals, can hardly be "compelling government interests" justifying content-based bans on certain kinds of speech, at least if the "compelling" threshold is to have any meaning. And the potential consequences of accepting this sort of justification for restricting speech are both clear and dire: The same rationale, after all, would easily justify bans on TV broadcasts that warn of cyberspace privacy risks, since such speech even more directly frightens consumers away from e-commerce and other Internet use.

Furthermore, if this is really such a great concern—which is far from clear, given the explosive growth of e-commerce even in the absence of noncontractual information privacy speech restrictions—it stands to reason that many Internet businesses would invest a lot of effort into preventing such consumer alienation: They'll promise not to communicate consumer information, set up enforcement mechanisms aimed at giving consumers confidence that such promises will be kept, distribute software that helps protect people's privacy through technological means, and so on. I'm not sure whether these tools would work quite as well as a total ban on speech about customers, but I suspect they would eventually go a long way towards assuaging consumer fears, precisely because online businesses would (by hypothesis) have such an economic stake in reassuring consumers.[275] And the availability of these tools further undercuts the case for restricting First Amendment rights in order to protect e-commerce.[276]

---

274. *Cf. generally* Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995).

275. On the other hand, if one believes that online businesses are investing little in reassuring consumers about cyber-privacy, this would be pretty strong evidence that consumers aren't really being frightened away from e-commerce by the millions, and that e-commerce can survive quite well without speech restrictions. *See also* Cohen, *supra* note 10, at 1424 (suggesting that autonomy values "require that we forbid data-processing practices . . . that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or genetic desirability"—a radical proposal indeed, given that rational people routinely rank potential commercial partners based on their financial desirability).

276. *Cf.* Reno v. ACLU, 521 U.S. 844, 885 (1997) (rejecting on similar though slightly different grounds a similar argument in support of restrictions on sexually themed speech). Thus, while I agree that "we routinely prohibit certain *uses* of gathered information that we deem inconsistent with shared notions of human dignity and equality," such as "race-based classification by private parties in virtually every aspect of commercial life," Cohen, *supra* note 10, at 1420 (emphasis

D. *Preventing Misconduct and Crime*

1. *Discrimination.*

Speech that reveals some kinds of information about people may make it easier for the listeners to act illegally or supposedly unfairly towards those people. One commonly given example is the risk that certain health-related information might fall into the hands of your health insurance company. "Say that the insurance company learns that you eat a lot of pizza and steak, and therefore concludes that you'll probably have higher cholesterol and a higher risk of heart disease," the argument goes; "it might then raise your rates." Another example is the risk that information about people's past crimes, alcoholism, or drug abuse will become known to employers, who will then refuse to hire these people.[277]

I can certainly see why people might be offended by their insurance company "snooping" on them this way. I can also see why it might be in the unhealthy eaters' financial interest (and I should mention that I love meat and cheese) not to be identified as such, so they can be subsidized by the healthy eaters with whom they pool their risk.[278] Similarly, closet smokers would prefer, if possible, that life insurance companies not be able to identify them as smokers. But the question is not just whether the communication of this information is offensive or financially costly to its subjects, but rather whether the government may suppress such communication.

If discrimination in insurance based on the insureds' eating habits is legal, as it is with respect to smoking habits, then it's hard to see how the risk of such lawful discrimination can justify restricting speech.[279] True, one's buying habits are not a perfect proxy for one's eating habits (maybe the buyer is a healthy eater who is buying the pizza entirely for his roommate), but insurance is all about using imperfect but lawful predictors. Being above twenty-five and being a good student don't perfectly predict whether someone will drive safely; smoking and being older don't perfectly predict whether someone will die soon; but virtually nothing perfectly predicts anything else. Likewise, many employers might consider a person's criminal

---

added), this by no means shows that we can prohibit communications of information. Discriminatory decisions that use certain information are not protected by the First Amendment. Speech that communicates information is protected by the First Amendment.

277. *See, e.g.*, James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 324 (1975) ("Revealing a pattern of alcoholism or drug abuse can result in a man's losing his job or make it impossible for him to obtain insurance protection . . . .").

278. *Cf.* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 395, 399 (1978) (more generally discussing people's desire to conceal discreditable information about themselves).

279. *See* U.D. Registry, Inc. v. California, 40 Cal. Rptr. 2d 228, 232-33 (Ct. App. 1995) (striking down an information privacy speech restriction that "seeks to limit the free flow of information for fear of its misuse by landlords" on the grounds that such a "paternalistic approach" is an impermissible ground for restraining either commercial or noncommercial speech).

record, alcoholism, or drug abuse relevant to whether they should entrust their property, their clients' well-being,[280] or a $100 million oil tanker to that person.

But even if the government outlaws discrimination based on insureds' eating habits, or discrimination based on a person's alcoholism, drug use, or criminal past,[281] the basic First Amendment rule is that while the government may restrict conduct, it generally can't restrict speech simply because some people may at some time be moved by the speech to act illegally.[282] The law has plenty of tools to fight such discrimination directly. They are not perfect tools, but under the First Amendment the government may not try to compensate for their imperfection by suppressing speech. The government may not suppress advocacy of discrimination based on race, criminal history, alcoholism, drug use, or pizza consumption, even though such advocacy may lead some people to actually engage in such discrimination. Likewise, the government may not suppress speech about particular people's criminal history, alcoholism, drug use, or pizza consumption, even though such speech may lead some people to engage in the discrimination.

2. *Fraud and violent crime.*

In a few cases, revealing certain information about people may make it easier for others to defraud them or even to commit violent crimes against them. Thus, LEXIS/NEXIS was faulted for putting people's social security numbers in a searchable online database; market pressure promptly led it to change its policy.[283] Likewise, the authors of the anti-abortion *Nuremberg Files* Web site were found civilly liable for, among other things, putting online the names, addresses, and other personal and family information about abortion providers.[284] A few disclosure tort cases have also punished the publication of the identity of witnesses who were vulnerable to attack by the criminals.[285]

---

280. Employers not only have moral and business reasons to make sure that they don't hire people who might abuse their customers, but legal reasons, too: A negligent failure to discover that an employee has a criminal record may lead to liability for negligent hiring if the employee later attacks a customer. *See, e.g.*, Carlsen v. Wackenhut Corp., 868 P.2d 882, 888 (Wash. App. 1994).

281. *See* N.Y. CORR. LAW §§ 752, 753 (generally barring employment discrimination based on criminal record); WISC. STAT. ANN. §§ 111.31, 111.32 (same).

282. *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444 (1969).

283. *See* Kang, *supra* note 28.

284. *See* Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists, 41 F. Supp. 2d 1130 (D. Ore. 1999).

285. *See* Capra v. Thoroughbred Racing Ass'n of North America, Inc., 787 F.2d 463 (9th Cir. 1986) (name of person in federal witness protection program); Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556 (Ct. App. 1988) (name of crime victim and witness where the criminal was still at large).

Under what circumstances the government may restrict speech that facilitates the commission of crime is a difficult and so far largely uninvestigated question.[286] It arises in many cases which have nothing to do with revelation of personal information, because personal information is just one of many kinds of information that can make it easier for people to commit crimes. The most prominent recent case that upheld a restriction on crime-facilitating speech involved a lawsuit against the publisher of a murder-for-hire manual.[287] The most prominent recent case striking down such a restriction involved a scientist trying to put his source code on a Web site, contrary to arms export laws.[288] The most prominent recent legislation aimed at such speech was a ban on certain online speech that described bombmaking techniques.[289] And the most famous cases that implicate this issue are the classic hypothetical of the publication of the sailing dates of troopships and the injunction against the publication of information about building an H-bomb.[290]

Moreover, even crime-facilitating speech that's focused on particular targets may involve information that few would consider especially private: For example, if a criminal is still at large, knows what a witness looks like, and would like to kill her in order to silence her, publicizing the name of the small business at which the witness works—hardly intimate information—may jeopardize her life almost as much as publishing her home address would. Similarly, if we're concerned about speech that facilitates fraud or theft, publishing information about a business's security vulnerabilities or a list of the business's computer passwords may create as much risk of fraud as publishing a person's social security number would.

I will not try to resolve this question here, but only want to offer three observations. First, the fact that speech facilitates crime doesn't always justify restricting the speech (even if it sometimes might): Consider, for instance, normal chemistry books, which may be used by criminals to learn how to make explosives,[291] or detective stories that describe particularly effective ways to commit a crime.

---

286. *See* U.S. Department of Justice, 1997 Report on the Availability of Bombmaking Information, *available at* <http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html>; KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE (1989); Eugene Volokh, *Crime-Facilitating Speech* (in progress).

287. *See* Rice v. Paladin Press, 128 F.3d 233 (4th Cir. 1997).

288. *See* Bernstein v. United States Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *reh'g en banc granted*, 1999 U.S. App. LEXIS 24324.

289. Pub. L. No. 106-54, sec. 2(a), *amending* 18 U.S.C. § 842 (enacted Aug. 17, 1999).

290. Near v. Minnesota, 283 U.S. 697, 716 (1931); United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), *appeal dismissed as moot*, 610 F.2d 819 (7th Cir. 1979). These cases (and to some extent *Bernstein*) involved speech that may facilitate foreign attack on the United States, rather than crime, but the principle is quite similar.

291. *See, e.g.*, U.S. Department of Justice, *supra* note 286 (listing a chemistry book from the respected Telford Press and books on explosives from the U.S. Bureau of Mines and the Associa-

Second, the strongest argument for restricting speech that reveals crime-facilitating personal information is that the speech facilitates crime, not that it reveals personal information. It is therefore probably most useful to analyze such speech as a kind of crime-facilitating speech, rather than as a specimen of revelation of personal data.

Third, as *Florida Star v. B.J.F.* held, the crime facilitation concern at most supports narrow restrictions on the particular kinds of speech that materially risk facilitating crime.[292] Whatever support there may be for a general right to suppress either speech that reveals embarrassing personal information or speech that reveals information about a person's purchases, the fact that a few kinds of such speech may facilitate crime can't justify these broad restrictions.

CONCLUSION

This article has made three arguments. First, despite their intuitive appeal, restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied. There may possibly be room for restrictions on revelations that are both extremely embarrassing and seem to have virtually no redeeming value, such as unauthorized distribution of nude pictures or possibly the publication of the names of rape victims, and perhaps for speech that makes it substantially easier for people to commit crimes against its subjects. Even these, though, pose significant doctrinal problems.

Second, expanding the doctrine to create a new exception may give supporters of information privacy speech restrictions much more than they bargained for. All the proposals for such expansion—whether based on an intellectual property theory, a commercial speech theory, a private concern speech theory, or a compelling government interest theory—would, if accepted, become strong precedent for other speech restrictions, including ones that have already been proposed. The analogies between the arguments used to support information privacy speech restrictions and the arguments used to support the other restrictions are direct and powerful. And accepting the principles that the government should enforce a right to stop others from speaking about us and that it's the government's job to create "codes of fair information practices" controlling private parties' speech may shift courts

---

tion of Australian State Road Authorities among sources "useful to individuals bent upon constructing bombs and other dangerous weapons").

292. *Cf.* Florida Star v. B.J.F., 491 U.S. 524, 537, 539 (1989) (acknowledging the concern about protecting "the physical safety of [rape] victims, who may be targeted for retaliation if their names become known to their assailants," but concluding that the law banning the publication of the names of rape victims was too broad); *id.* at 542 (Scalia, J., concurring in part and concurring in the judgment) (explicitly concluding that the interest in protecting victims' physical safety would justify only a law that applied to cases where the attacker was still at large).

and the public to an attitude that is more accepting of government policing of speech generally. The risk of unintended consequences thus seems to me quite high.

Third, this leaves people who are trying to make up their mind about information privacy speech restrictions with several options:

Some people can wholeheartedly embrace some of the arguments for these restrictions, precisely because these arguments would help create precedent for cutting back certain free speech protections. Thus, for instance, those who argue that the First Amendment should primarily cover speech that fairly directly furthers self-government[293] may want to adopt information privacy speech restrictions as their poster child. These restrictions are popular, they can to a large extent be defended using the "First Amendment only strongly protects speech relevant to self-government" theory, they are hard to defend under a more inclusive theory, and they can therefore produce substantial support for the theory among those who like the restrictions.

Others, who generally oppose any broad diminution of free speech protections but who think information privacy speech restrictions must be upheld, can try to set forth their proposed new exception and its supporting arguments as carefully and narrowly as possible. I hope their attempt to craft such a well-cabined, narrow rationale for any such new exception will be helped by this Article, which highlights some of the analogies that generally pro-speech-restriction forces might use to expand any exception that is created. Maybe with a very carefully drawn exception, my fears about the unintended consequences of recognizing such exceptions won't come to pass.

Still others may reluctantly conclude that the risk is just too great. We protect a good deal of speech we hate because we fear that restricting it will jeopardize the speech we value.[294] Some people may likewise conclude that it's better to protect information privacy in ways other than speech restriction—through contract, technological self-protection, market pressures, restraints on government collection and revelation of information, and social norms—than to create a new exception that may eventually justify many more restrictions than the one for which it is created. Perhaps the Michigan Supreme Court's decision 100 years ago, in response to the Brandeis & Warren privacy tort proposal, was correct:

> This "law of privacy" seems to have obtained a foothold at one time in the history of our jurisprudence, —not by that name, it is true, but in effect. It is evidenced by the old maxim, "The greater the truth, the greater the libel," and the

293. *See, e.g.*, Owen M. Fiss, *Free Speech and Social Structure*, 71 IOWA L. REV. 1405, 1411 (1986); Cass R. Sunstein, *Free Speech Now*, 59 U. CHI. L. REV. 255, 263 (1992).

294. *See* Communist Party of the United States v. Subversive Activities Control Bd., 367 U.S. 1, 137 (1961) (Black, J., dissenting) ("I do not believe that it can be too often repeated that the freedoms of speech, press, petition and assembly guaranteed by the First Amendment must be accorded to the ideas we hate or sooner or later they will be denied to the ideas we cherish.").

> result has been the emphatic expression of public disapproval, by the emancipation of the press, and the establishment of freedom of speech, and the abolition in most of our States of the maxim quoted, by constitutional provisions . . . .
>
> We do not wish to be understood as belittling the complaint. We have no reason to doubt the feeling of annoyance alleged. Indeed, we sympathize with it, and marvel at the impertinence that does not respect it. We can only say that it is one of the ills that, under the law, cannot be redressed. [295]

All three of these approaches have their strengths; the one approach, though, that I think is entirely unsound is to simply ignore the potential free speech consequences. The speech restrictions that courts validate today have implications for tomorrow. Only by considering these implications can we properly evaluate the true costs and benefits of any proposed information privacy speech restriction.

295. Atkinson v. John E. Doherty & Co., 80 N.W. 285, 289 (Mich. 1899). *Atkinson* involved speech that today might give rise to a right of publicity claim, but in this quotation the court was discussing the Warren & Brandeis right of privacy, which was primarily focused on what today would be called the disclosure tort.