Before the
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC

In the Matter of:	)	
	)	
Developing the Administration's	)	Docket No. 180821780-8780-01
Approach to Consumer Privacy	)	

Comments of Prof. Steven M. Bellovin

via electronic filing
November 7, 2018

Thank you for the opportunity to submit comments on *Developing the Administration's Approach to Consumer Privacy*. I write to suggest that the current standard approach, "notice and consent", is fatally flawed and cannot serve as the basis for protecting privacy in the future. A different approach is needed today, as well as more research.

I am the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University; I am also an affiliate faculty member at Columbia Law School and am currently a Visiting Scholar at the Center for Law and Information Policy at Fordham University Law School.[1] I have also been a researcher at Bell Labs and AT&T Labs; I have served as Chief Technologist for the Federal Trade Commission and as the Technology Scholar at the Privacy and Civil Liberties Oversight Board.[2] My primary technical expertise is in security and privacy; for the last several years, my focus has been on legal aspects of technology, and I have published a number of law review articles in this area. All opinions expressed are personal and do not necessarily represent the opinions of any organization I am now or have been associated with.

I The Problem with Notice and Consent

Modern approaches to privacy go back to the 1960s. The best known work is Alan Westin's classic 1967 book,[3] which largely reflects the work of the Committee on Science and Law of the Association of the Bar of the City of New York.[4] He noted the importance of consent:[5]

> A central aspect of privacy is that individuals and organizations can determine for themselves which matters they want to keep private and which they are willing—or need—to reveal.

He also noted that it was crucial to realize that consent is limited to a particular situation, and should not be seen as blanket permission to disseminate information:[6]

> Finally, it should be recognized that consent to reveal information to a particular person or agency, for a particular purpose, is not consent for that information to be circulate to all or used for other purposes. The individual may consent to tell things to his teacher or professor that ought not be circulated as part of student records without the student's consent. Information given to life-insurance companies, credit agencies, survey researcher, or government regulatory and welfare agencies ought not to be shared, in ways that identify the particular individual, without notice of the additional use and consent to it. Unless this principle of consent is well understood and accepted as the controlling principle for information flow in a data-stream society, we will be in for serious problems of privacy in the future.

Donald Michael worried about the effects of having too much private data available:[7]

> Private information about a person may exist which is ethically or legally restricted to those who have a legitimate right to it. Such information, about a great portion of our population, exists in business, medical, government, and political files, and in the form of psychological tests, private and government job application histories, federal and state income tax records, draft records, security and loyalty investigations, school records, bank records, credit histories, criminal records, and diaries. Each day more of these records are translated from paper to punchcards and magnetic tapes. In this way they are made more compact, accessible, sometimes more private, and, very importantly, more centralized, integrated, and articulated. The results are more complete records on each individual and a potential for more complete cross-correlations. The would-be invader who knows about these centralized or clustered inventories need not search for sources, and therefore he may be much more inclined to examine the records than if a major search for the sources of information were necessary.

[1] Affiliations listed for identification purposes only.

[2] My standard biography is at `https://www.cs.columbia.edu/~smb/bio.html`; my CV is at `https://www.cs.columbia.edu/~smb/cv.pdf`.

[3] Alan F. Westin. *Privacy and Freedom*. New York: Atheneum, 1967.

[4] *Id.* at ix.

[5] *Id.* at 373.

[6] *Id.* at 375.

[7] Donald N. Michael. "Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy". In: *George Washington Law Review* 33 (1964), p. 270. URL: `https://heinonline.org/HOL/P?h=hein.journals/gwlr33&i=284`, at 274.

and worried about people surrendering their data too easily:[8]

> [W]e can expect a great deal of information about the social, personal, and economic characteristics of individuals to be supplied voluntarily—often eagerly—in order that, wherever they are, they may have access to the benefits of the economy and the government.

Arthur R. Miller wrote extensively on the legal aspects of privacy,[9] and testified on it before a Senate subcommittee.[10] He spoke explicitly of the need for openness and correctness:[11]

> To insure the accuracy of the Center's files, an individual should have access to any stored information concerning him and an opportunity to challenge its accuracy. Perhaps a print-out of a person's record can be sent to him once a year. This suggestion obviously is vulnerable to a number of criticisms. It is expensive, some federal agencies will argue that the value of certain information will be lost if it is disclosed that the government has it, and the suggestion *might* produce a flow of squabbles, many of them petty, with the Data Center, that would entail costly and debilitating administrative proceedings. Nonetheless, the right of citizen to be protected against governmental dissemination of misinformation is so important, some price must be paid preserve it. The monetary cost of informing the public could be reduced by forwarding the print-out with one of the numerous governmental communications that are sent individuals every year. Alternatively, citizens could be given access to their own files on request, perhaps through a network of remote terminals in government buildings. Legitimate governmental secrecy could be preserved and disputes over file content could be reduced if the information in the Center, and access to it, were arranged hierarchically according to content and an individual received only that part of the file that is accessible to anyone outside the agency that collected it.

However, he warned about relying too much on consent as a way to protect privacy:[12]

> A final note on access and dissemination. Excessive reliance should not be placed on what too often is viewed as a universal solvent—the concept of consent. How much attention is the average citizen going to pay to a governmental form requesting consent to record or transmit information? It is extremely unlikely that the full ramifications of the consent will be spelled out in the form; if they were, the document probably would be so complex that the average citizen would find it incomprehensible. Moreover, in many cases the consent will be coerced, not necessarily by threatening a heavy fine or imprisonment, but more subtly by requiring consent as a prerequisite to application for a federal job, contract, or subsidy.

This warning was prescient.

A few years later, the groundbreaking work of these and other pioneers was one of the foundations for a very important publication, a report by an advisory committee to the then-extant Department of Health, Education, and Welfare.[13] This report set forth what have become known as the Fair Information Practice Principles (FIPP):[14]

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

[8] Michael, *supra* note 7, at 278.

[9] *See, e.g.*, Arthur R. Miller. "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society". In: *Michigan Law Review* 67.6 (1969), pp. 1089–1246. ISSN: 00262234. URL: http://www.jstor.org/stable/1287516

[10] *Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate, 90th Congress, First Session*. Government Printing Office, Mar. 1967. URL: http://hdl.handle.net/2027/osu.32437121556241, at 66.

[11] *Id.* at 77.

[12] *Id.* at 78.

[13] *See generally* Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and the Rights of Citizens*. DHEW Publication, no. (OS) 73-94. United States Deptartment of Health, Education, and Welfare, 1973. URL: https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[14] *Id.* at xx.

- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

These five principles have formed the basis for all modern privacy regulation, including the U.S. Privacy Act of 1974[15] and the European Union's General Data Protection Regulation.[16]

Note the third bullet: consent for each use. Consent, in fact, is part of the very definition of privacy in technical fora:[17]

> 1. The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. (See: HIPAA, personal information, Privacy Act of 1974. Compare: anonymity, data confidentiality.)
>
> 2. "The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed."

[Citations omitted.]

In fact, these definitions draw on Westin's: "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."[18] The problem, though, is that in today's world, consent no longer works. There is far too much data, the collectors are opaque to ordinary citizens, and new technologies render the very concept of "purpose" meaningless. Our "data shadow"[19] is too large; it is not possible to control it.

The first problem is the collection of data. All but unknown to most citizens, so-called data brokers[20] collect vast amounts of data on individuals.[21] Their activities are not secret; indeed, Federal Trade Commission members have warned about their data collection practices and volume: "[Acxiom's] databases contain information about 700 million consumers worldwide with over 3000 data segments for nearly every U.S. consumer."[22] Despite this, most people are unaware of these companies or their practices: "Much of this activity takes place without consumers? knowledge."[23] People are also unaware of their ability to see the data collected about them:[24]

> In the past Acxiom has allowed consumers to see the part of their dossier gathered from public documents, but the request process is onerous. Anyone interested has to send in their Social Security number, date of birth, driver's license number, current address, phone number and email address, as well as a $5 check. Few have cleared this hurdle. Between 2009 and mid 2012 when they sent information about this process to a Congressional panel, between 77 and 342 people had asked to see their files every year, with just two to 16 annually providing enough information to get access to their file.

---

[15] Privacy Act, 5 U.S.C. §552a (1974).

[16] EU. *General Data Protection Regulation*. Regulation (EU) 2016/679. May 4, 2016. URL: https://gdpr-info.eu/.

[17] R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949. Aug. 2007. URL: http://www.rfc-editor.org/rfc/rfc4949.txt, at 233.

[18] Westin, *supra* note 3, at 7.

[19] *Id.*

[20] Data brokers are distinct from credit bureaus in a number of different ways. Most crucially, the latter are regulated by the Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq*.

[21] *See* Natasha Singer. "Acxiom, the Quiet Giant of Consumer Database Marketing". In: *New York Times* (June 16, 2012). URL: https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html. *See generally* Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability*. May 2014. URL: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf for a wealth of information on data brokers, what they do, and what the risks are.

[22] *Id.* at 8.

[23] *Id.* at 49.

[24] Adam Tanner. "Finally You'll Get To See The Secret Consumer Dossier They Have On You". In: *Forbes* (June 25, 2013). URL: https://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/#19ff366d521e.

Acxiom had plans to ease the process;[25] the portal that allows access to at least some data[26] is described as a way to "[a]ccess the many data points from Acxiom and our partners that companies use to deliver your personalized ads and offers." The purpose of the portal is to help "marketers create personalized offers that match your lifestyle and buying habits."[27] It is hard to see this as informed consent within the spirit of the FIPPs. If nothing else, it is consent for just one use: targeted advertising.

The second problem today is that there are many more ways in which data can be collected about people. Search engines know which links you click on. In part, they use that to improve their results—"for query X, more people preferred the third answer"—but the information is also used to build behavior and interest profiles on individuals. Web sites not only track you directly when you visit their sites, they purchase other data about you[28] and use technical means to track you elsewhere.[29] All of this information is, of course, disclosed in privacy policies; however, few people actually read them. In fact, according to a study by McDonald and Cranor, the time and opportunity cost to do so are prohibitive:[30]

> [U]sing the point estimate of 244 hours per year to read privacy policies per person means an average of 40 minutes a day. This is slightly more than half of the estimated 72 minutes a day people spend using the Internet.

They estimate the opportunity cost of this activity at over $3,500 per year.[31] It is perhaps the supreme irony that Chief Justice Roberts himself does not pay attention to this fine print.[32] A PCAST report to President Obama said it well: "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[33]

Furthermore, privacy policies are often unhelpful. Reidenberg et al. point to vague statements, *e.g.*, "We may collect personal information and other information about you from business partners, contractors and other third parties."[34] Users do not know if information will be collected, from whom, or what that information might be. Some of the issue appears to be lack of regulatory oversight; companies whose privacy policies are governed by regulation are significantly less vague.[35] Furthermore, even experts can misunderstand what is actually said.[36]

An FTC report noted that mobile devices are worse.[37]

> One theme was that consumers do not know or understand current information collection and use practices occurring on mobile devices. According to one participant, because consumers are unaware that many

[25] Tanner, *supra* note 24.

[26] *See* https://www.aboutthedata.com/portal.

[27] *Id.*

[28] The *Wall Street Journal*'s privacy policy (https://www.dowjones.com/privacy-policy/) says, in part, "We may receive Other Information about you from third parties, including, for example, demographic data, social media account number, information about your interests, and information about your activities on other websites."

[29] "Through third party analytics providers, ad networks, and advertisers, we can track your online activities over time and across third party websites, apps and devices, by obtaining information through automated means.

"...This information, along with information we gather when you log in, can be used to understand use across sites and devices to help improve our products, remember your preferences, provide content recommendations, and show you advertisements on the Dow Jones Services or other third party websites and apps that may be tailored to your individual interests." *Id.*

[30] Aleecia M McDonald and Lorrie Faith Cranor. "The cost of reading privacy policies". In: *ISJLP* 4 (2008), p. 543. URL: https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc4&i=563, at 563.

[31] *Id.* at 564.

[32] Debra Cassens Weiss. "Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print". In: *ABA Journal* (Oct. 20, 2010). URL: http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.

[33] President's Council of Advisors on Science and Technology. *Big Data and Privacy: A Technological Perspective*. Report to the President. May 2014. URL: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

[34] Joel R. Reidenberg, Jaspreet Bhatia, Travis D. Breaux, and Thomas B. Norton. "Ambiguity in Privacy Policies and the Impact of Regulation". In: *The Journal of Legal Studies* 45.S2 (2016), S163–S190. DOI: 10.1086/688669. eprint: https://doi.org/10.1086/688669. URL: https://doi.org/10.1086/688669, at s166.

[35] *Id.* at s181.

[36] Joel R. Reidenberg et al. "Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding". In: *Berkeley Technology Law Journal* 30.1 (2015), pp. 39–68. URL: http://scholarship.law.berkeley.edu/btlj/vol30/iss1/3.

[37] *See* Federal Trade Commission. *Mobile Privacy Disclosures: Building Trust Through Transparency*. Feb. 2013. URL: https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf, p. 10. (Internal citations omitted.)

> of these practices are taking place, they do not look for options providing them with control over such practices. Another participant noted that when made aware of these practices, consumers typically are surprised and view the practices as underhanded. Participants noted that when disclosures are made, consumers often do not understand them.

The report also noted the danger of location collection:[38]

> Third, mobile devices can reveal precise information about a user's location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers. Indeed, companies can use a mobile device to collect data over time and 'reveal[] the habits and patterns that mark the distinction between a day in the life and a way of life.' Even if a company does not intend to use data in this way, if the data falls in the wrong hands, the data can be misused and subject consumers to harms such as stalking or identity theft

Mobile devices do create voluminous amounts of location data. Speaking of cell site location information (CSLI) the Supreme Court itself has recognized that this is not shared voluntarily with phone companies:[39]

> Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. [citations omitted]

Some apps are far worse. It is undoubtedly convenient to use a phone for turn-by-turn directions; however, the service provider may obtain continuous location information during the drive.[40]

More new privacy dangers are posed by the so-called "Internet of Things":[41]

> Cars, door locks, contact lenses, clothes, toasters, refrigerators, industrial robots, fish tanks, sex toys, light bulbs, toothbrushes, motorcycle helmets—these and other everyday objects are all on the menu for getting "smart." Hundreds of small start-ups are taking part in this trend—known by the marketing catchphrase "the internet of things".

And these devices all pose risks: "There's just one catch, which often goes unstated: If their novelties take off without any intervention or supervision from the government, we could be inviting a nightmarish set of security and privacy vulnerabilities into the world. And guess what. No one is really doing much to stop it."[42] Most of these devices lack screens, keyboards, and mice. If it is hard to know what a computer or phone is doing, how can one tell the behavior of an Internet-connected hair brush[43] or thermometer?[44]

[38] FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency*, *supra* note 37, at 3.

[39] Carpenter v. United States, 138 S. Ct. 2206, 2220 (U.S. June 22, 2018).

[40] It is in fact unclear, even to technically sophisticated users, what location information is shared and when; *see* Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie Pell. "It's Too Complicated: How the Internet Upends *Katz*, *Smith*, and Electronic Surveillance Law". In: *Harvard Journal of Law and Technology* 30.1 (Fall 2016), pp. 1–101. URL: http://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf, at 83–88 ("Whether a mapping application is sending its location to the application provider frequently, occasionally, or never need not manifest itself in the behavior of the software.")

[41] Farhad Manjoo. "A Future Where Everything Becomes a Computer Is as Creepy as You Feared". In: *New York Times* (Oct. 10, 2018). URL: https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html.

[42] *Id.*

[43] John Kell. "L'Oreal's 'Smart' Hairbrush Wants to Help Solve a Huge Beauty Problem". In: *Fortune* (Jan. 4, 2017). URL: http://fortune.com/2017/01/03/loreal-smart-hairbrush-ces/.

[44] *See* Sapna Maheshwari. "This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise". In: *New York Times* (Oct. 23, 2018). URL: https://www.nytimes.com/2018/10/23/business/media/fever-advertisements-medicine-clorox.html. This particular use is innocuous, in that only zip code data is used for targeted advertising. But the collection mechanism exists, and future companies may not be as ethical.

The reason for all of this tracking is, of course, to monetize the information, and in particular monetize it by using it for targeted advertising. It is no surprise that two of the most successful Internet companies, Google and Facebook are also two of the biggest collectors of personal information; together, they control a majority of the online advertising market.[45] In fact, more than half of U.S. advertising is online,[46] and hence driven by personal information.

Advertising has been called "the original sin of the Internet":[47]

> I have come to believe that advertising is the original sin of the web. The fallen state of our Internet is a direct, if unintentional, consequence of choosing advertising as the default model to support online content and services. Through successive rounds of innovation and investor storytime, we've trained Internet users to expect that everything they say and do online will be aggregated into profiles (which they cannot review, challenge, or change) that shape both what ads and what content they see. Outrage over experimental manipulation of these profiles by social networks and dating companies has led to heated debates amongst the technologically savvy, but hasn't shrunk the user bases of these services, as users now accept that this sort of manipulation is an integral part of the online experience.

There are, of course, benefits to an ad-supported Internet: it makes it accessible to more people.[48] Facebook thus brags that "It's free and always will be."[49] But the cost in privacy is considerable: Internet ads are perceived to work best when they're highly targeted; this in turn means that advertising companies must collect as much information as they can about their users. That in turn has meant tracking them across sites, using tools such as "web beacons"[50] and the ubiquitous Facebook "like" buttons. These in turn make a mockery of user consent: if you can't see a web beacon—by definition, they're often invisible—and if you don't know that the existence of a Facebook "like" button on a page means that Facebook can track your visit there, it is impossible to control your information.

There are other facets of Internet advertising that render useless any attempts by Internet users to understand who has their data. Few Internet ads are actually displayed by the hosting sites; instead, they come from Internet advertising companies, such as Google's Doubleclick unit.[51] This is indeed acknowledged by the privacy policies of many media companies. The *New York Times*' privacy policy says[52]

> Some of the services and advertisements included in the NYT Services, including on NYTimes.com and within our mobile apps, are delivered or served by third-party companies, which may collect information about your use of the NYT Services.
>
> These companies place or recognize cookies, pixel tags, web beacons or other technology to track certain information about our NYT Services website users. For example, in the course of serving certain advertisements, an advertiser may place or recognize a unique cookie on your browser in order to collect certain information about your use of the NYT Services. For another example, an advertiser or ad server may also be able to collect your device's unique identifier in the course of serving an ad. In many cases, this information could be used to show you ads on other websites based on your interests.
>
> *We do not have access to, nor control over, these third parties' use of cookies or other tracking technologies or how they may be used.* [emphasis added]

[45] Rani Molla. "Google's and Facebook's share of the U.S. ad market could decline for the first time, thanks to Amazon and Snapchat". In: *Recode* (Mar. 19, 2018). URL: https://www.recode.net/2018/3/19/17139184/google-facebooks-share-digital-advertising-ad-market-could-decline-amazon-snapchat.

[46] Lucas Shaw. "Google, Facebook Lead Digital's March to Half of U.S. Ad Market". In: *Bloomberg* (Sept. 20, 2018). URL: https://www.bloomberg.com/news/articles/2018-09-20/google-facebook-lead-digital-s-march-to-half-of-u-s-ad-market.

[47] Ethan Zuckerman. "The Internet's Original Sin". In: *The Atlantic* (Aug. 14, 2014). URL: https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

[48] *Id.* ("Charging users for the service would have blocked most of our potential customers—most of the world still doesn't have a credit card today, and fewer did in 1995.")

[49] *See* https://www.facebook.com.

[50] *See* https://iapp.org/resources/article/web-beacon/ ("Also known as a web bug, pixel tag or clear GIF, a web beacon is a clear graphic image (typically one pixel in size) that is delivered through a web browser or HTML e-mail.").

[51] *See e.g.*, Dan Wallach, FTC working *The Big Picture: Comprehensive Online Data Collection* transcript, December 6, 2012, Session 1, at 22, https://www.ftc.gov/sites/default/files/documents/videos/big-picture-comprehensive-online-data-collection-session-1/4/121206bigpicturept1.pdf.

[52] https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy

In other words, to protect your privacy you must know the policies of not just the sites you visit, but the policies of their advertisers as well. Furthermore, it is not just a single layer; often, the primary advertising site will redirect you to a third, which can send you to a fourth, *ad nauseum*.[53] Even advertisers who do not participate in the actual ad display learn something about users, via a bidding process:[54]

> But Rubicon is not just a sales platform for Web site operators. It's an analytics system that uses consumer data to help sites figure out how much their visitors are worth to advertisers.
>
> Most sites, Mr. Addante explains, compile data about their own visitors through member registration or by placing bits of computer code called cookies on people's browsers to collect information about their online activities. To those first-party profiles, Rubicon typically adds details from third-party data aggregators, like BlueKai or eXelate, such as users' sex and age, interests, estimated income range and past purchases. Finally, Rubicon applies its own analytics to estimate the fair market value of site visitors and the ad spaces they are available to see.
>
> The whole process typically takes less than 30 milliseconds.

The dynamic nature of the the advertising ecosystem makes setermining which sites are showing you ads—in other words, which sites' privacy policies you need to read—is quite daunting, even for experts. This is best seen by noting how hard it is for even well-meaning web sites to eliminate obnoxious (and probably fraudulent) ads[55]:

> Within about an hour we had successfully replicated the issue and pinpointed the source. Our AdOps team moved quickly to alert the vendor whose network was being used to serve the ad, and we blocked the source of the issue in Google's tools. By the end of the day we felt we had successfully blocked the ad and had stopped receiving reports of redirects for the day. Whoever was behind the ad, however, kept finding ways into the system throughout the week on Vox Media sites and many others around the web. Our tools for blocking this require us to identify the source of each malicious ad and block it, which is reactive and not preventative.

In other words, it took a team of professionals an hour to find the actual source of one ad, but the offender—that is, a different web site—kept moving to different places. For our purposes, what matters is that each such site could have a different privacy policy, and that new sites are appearing constantly. An ordinary users would have no hope of finding even the immediate ad source, let alone the identities of any intermediaries.

Some sites explicitly list their possible partners. The transparency is good, but the numbers can be shocking. PayPal, for example, lists a huge number of sites with which they will sometimes share information.[56] From the site, it is clear that many of the entries are country-specific, and that many are unquestionably necessary, either to carry out their services or to comply with laws and regulations. But a fair number of companies are there for marketing or to "deliver personalised [sic] advertising".

The risks of tracking and dossier compilation go far beyond marketing. Recommendation engines are recommendation engines; they're agnostic to what they're suggesting. It may be something benign, such as what movie you might want to watch next. But it can also be used—and abused—to spread propaganda. Tufekci has argued that YouTube is a potent radicalizing engine: "It seems as if you are never 'hard core' enough for YouTube's recommendation algorithm. It promotes, recommends and disseminates videos in a manner that appears to constantly up the stakes. Given its billion or so users, YouTube may be one of the most powerful radicalizing instruments of the 21st century."[57] There do not appear to be malicious political intentions at play here, but there certainly could be. Apart from the widely reported "fake news" phenomena during the 2016 election, where invented stories spread rapidly on

[53] *See* Wallach, *supra* note 51.

[54] Natasha Singer. "Your Online Attention, Bought in an Instant by Advertisers". In: *New York Times* (Nov. 17, 2012). URL: https://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html.

[55] Winston Hearn. "Why ads keep redirecting you to scammy sites and what we're doing about it". In: *Vox Media* (Jan. 22, 2018). URL: https://product.voxmedia.com/2018/1/22/16902862/why-ads-redirect-to-giftcards-and-what-were-doing-to-secure-them.

[56] *See* https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list. There is an excellent visualization at https://rebecca-ricks.com/paypal-data/, though the date of the source data is not stated.

[57] Zeynep Tufekci. "YouTube, the Great Radicalizer". In: *New York Times* (Mar. 10, 2018). URL: https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

social media, an experiment—done with the cooperation of Facebook—showed that Facebook messages could affect voter turnout.[58] More ominously, in Myanmar the military apparently "turned the social network into a tool for ethnic cleansing, according to former military officials, researchers and civilian officials in the country."[59] More than 700,000 Rohingya have fled the country in fear of their lives.[60]

Finally, as Paul Ohm has argued, the very existence of these digital dossiers is itself a serious risk:[61]

> In my work, I've argued that these databases will grow to connect every individual to at least one closely guarded secret. This might be a secret about a medical condition, family history, or personal preference. It is a secret that, if revealed, would cause more than embarrassment or shame; it would lead to serious, concrete, devastating harm. And these companies are combining their data stores, which will give rise to a single, massive database. I call this the Database of Ruin.

As I have often argued in my work, something that does not exist cannot be stolen or otherwise misused.

Apart from ubiquitous, invisible collection of data, there is another technological development that has had a great effect on our privacy: machine learning.[62] Machine learning (ML), sometimes called AI or artificial intelligence",[63] relies on "training" the system with a large amount of data. The ML system finds patterns and, in effect, makes predictions. Thus, when Netflix suggests movies to a user, or Amazon says "people who bought this also bought this other thing", those suggestions are not the result of human reasoning and curation. Rather, the algorithm—more precisely, the algorithm plus the training data—have found correlations that users hopefully find useful.

Some people find these recommendations annoying and intrusive. "Many consumers appreciate having computers delve into their hearts and heads. But some say it gives them the willies, because the machines either know them too well or make cocksure assumptions about them that are way off base."[64] In one famous incident, Target used sales data that *correlated with* pregnancy to send targeted ads; they identified one teenage girl as pregnant before her parents knew.[65]

That these large databases exist is troubling enough from a privacy perspective. What makes them problematic, though, is that they are dual use: they are used both intrusively and to deliver desired results. When you type the name of a restaurant into Google, even if it is a very generic restaurant name, you will likely be shown the web site of the one near you. How? Google's algorithms take into account your IP address, which is correlated with your location,[66] and the fact that most people look for restaurants near where they are.

This, then, is the dilemma. The FIPPs state "There must be a way for an individual to find out what information about him is in a record and how it is used."[67] However, machine learning algorithms do not work that way. They do not provide any explanation for *why* a particular correlation exists and hence cannot say what in a particular record produced a given answer. It is therefore impossible to assert or deny that a particular datum was used for some purpose.

---

[58] Robert M. Bond et al. "A 61-million-person experiment in social influence and political mobilization". In: *Nature* 489 (Sept. 2012), 295 EP -. URL: http://dx.doi.org/10.1038/nature11421.

[59] Paul Mozur. "A Genocide Incited on Facebook, With Posts From Myanmar's Military". In: *New York Times* (Oct. 15, 2018). URL: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[60] *Id.*

[61] *See* Paul Ohm. "Don't Build a Database of Ruin". In: *Harvard Business Review blog network* (Aug. 23, 2012). URL: https://hbr.org/2012/08/dont-build-a-database-of-ruin. For a more detailed discussion of databases of ruin, *see also* Paul Ohm. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". In: *UCLA Law Review* 57 (2010). U of Colorado Law Legal Studies Research Paper No. 9-12, pp. 1701–1777. URL: https://heinonline.org/HOL/P?h=hein.journals/uclalr57&i=1713.

[62] *See* Hal Daumé. *A Course in Machine Learning*. Self-published. 2017. URL: http://ciml.info/ at 8 ("At a basic level, machine learning is about predicting the future based on the past. For instance, you might wish to predict how much a user Alice will like a movie that she hasn't seen, based on her ratings of movies that she has seen.")

[63] Artificial intelligence is a broad field, going back more than 60 years. Its goal is, roughly, to produce a computer that can think (whatever that means). Machine learning is one specific technology (more precisely, a set of technologies) for achieving AI. Because of how well it works, it is currently the most favored approach to achieving artificial intelligence; as a result, the two terms are often conflated.

[64] Jeffrey Zaslow. "If TiVo Thinks You Are Gay, Here's How to Set It Straight". In: *Wall Street Journal* (Nov. 26, 2002). URL: https://www.wsj.com/articles/SB1038261936872356908.

[65] Charles Duhigg. "How Companies Learn Your Secrets". In: *New York Times* (Feb. 16, 2012). URL: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[66] IP addresses—Internet Protocol addresses—are the Internet's analogue to phone numbers. For reasons beyond the scope of this note, IP addresses generally indicate one's rough locale—think of how, in the pre-cellular era, the area code and exchange of a phone number denoted the city. In both cases, the association is done for strong technical reasons.

[67] Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 13.

The advent of machine learning raises two more fundamental issues with the FIPPs: the entire scheme is based on the notion of protecting personally identifiable information (PII). Four of the five principles, in fact, explicitly refer to individual records. However, ML algorithms do not need to know someone's identity to invade privacy. The "My Tivo Thinks I'm Gay" incident[68] is just one example, but in principle, most recommendation algorithms do not need PII.[69] Furthermore, it is often possible to deanonymize records.[70]

Furthermore, these algorithms may be able to infer PII, even if none of the data used contains explicit identifying information. Consider a turn-by-turn map application. Over time, the location that someone frequently leaves from in the morning or returns to in the evening is likely their home address. Does this count as "a record of identifiable information" about a particular person? What if the PII is obtainable only by combining one highly revealing dataset with another that contains the actual identifiers?

II Data Security

The fifth principle in the FIPPs requires data security, to "prevent misuse of the data". This point is worth a separate discussion.

Empirically, our data is at great risk. Many large organizations have proven unable to protect themselves against attacks.[71] It is, of course, obvious that without data security, one cannot guard against theft and hence misuse of data. Similarly, unauthorized modification of records leads to incorrect data about individuals. In other words, even if security were not called out specifically, it is implicit in the other principles. The Federal Trade Commission has used this theory in becoming a de facto privacy regulator.[72] Using its powers under Section 5 of the Federal Trade Commission Act,[73] the FTC has often moved against companies with inadequate data security, on the grounds that such behavior is *a priori* unfair competition; additionally, if consumers are promised that their data will be protected, failure to do so can constitute deception.

There are two caveats, however. First, the Act gives the FTC authority over "[u]nfair methods of competition. . . and unfair or deceptive acts or practices."[74] Second, the offending behavior must be one that "causes or is likely to cause substantial injury to consumers." Both limitations are significant.

When can a security breach be considered an unfair or deceptive act or practice? The FTC has never issued any regulations on this; however, in the past, it has held that failure to adopt "reasonable and appropriate" measures was in itself unfair.[75] This standard has been upheld by the Third Circuit.[76] But the actual standards that companies must follow to avoid liability remain unclear: "The painful reality is that we lack broadly applicable, specific standards, partially because of the ugly complexity of the problem. It involves not just technical standards but also corporate executive decisionmaking and reevaluation of practices over time."[77]

The second issue is how to define "substantial injury". Traditionally, the FTC has held that "[m]onetary, health, and safety risks are common injuries considered 'substantial,' but trivial, speculative, emotional, and 'other more

[68] Zaslow, *supra* note 64.

[69] This may not be strictly true: PII may, in fact, be helpful. Some products are particularly appealing to certain demographics; knowledge of those could lead to more accurate suggestions.

[70] *See e.g.*, Michael Barbaro and Tom Zeller Jr. "A Face Is Exposed for AOL Searcher No. 4417749". In: *New York Times* (Aug. 9, 2006). URL: https://www.nytimes.com/2006/08/09/technology/09aol.html or Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *supra* note 61.

[71] *See, e.g.,* Mike Isaac and Sheera Frenkel. "Facebook Security Breach Exposes Accounts of 50 Million Users". In: *New York Times* (Sept. 28, 2018). URL: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html; Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.". In: *New York Times* (Sept. 7, 2017). URL: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; Brian Krebs. "Congressional Report Slams OPM on Data Breach". In: *Krebs on Security* (Sept. 16, 2016). URL: https://krebsonsecurity.com/2016/09/congressional-report-slams-opm-on-data-breach/.

[72] Daniel J Solove and Woodrow Hartzog. "The FTC and the new common law of privacy". In: *Colum. L. Rev.* 114 (2014), p. 583. URL: https://heinonline.org/HOL/P?h=hein.journals/clr114&i=617.

[73] Federal Trade Commission Act, 15 U.S.C. §45.

[74] 15 U.S.C. §45(a)(1).

[75] Solove and Hartzog, *supra* note 72, at 643.

[76] Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (2015).

[77] Merritt Baer and Chinmayi Sharma. "What Cybersecurity Standard Will a Judge Use in Equifax Breach Suits?" In: *Lawfare* (Oct. 20, 2017). URL: https://www.lawfareblog.com/what-cybersecurity-standard-will-judge-use-equifax-breach-suits.

subjective types of harm' are usually not considered substantial for unfairness purposes."[78] Courts have frequently held that mere disclosure of other information does not constitute harm.[79]

This standard is inadequate. Apart from the risk of sensitive theft via disclosure of private information, per the FIPPs the inability to control disclosure of information is itself a problem. If privacy is, at root, "[T]he right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment,"[80] undesired disclosure is by definition a privacy violation. However, the FTC may not have the authority to act.

III Analysis

We now revisit the five privacy principles originally spelled out[81] and see how they no longer work.

There must be no personal data record keeping systems whose very existence is secret. Few, if any, Internet companies are secret. That is, their existence is public, and at least some details about their data collection practices are known. Partly, this is out of necessity; California, a huge market, requires that privacy policies exist.[82] Nevertheless, though the information is available to those who know to look, very few people are aware of these companies; as noted, the role of online advertising intermediaries is very hard to determine, even for skilled users. Furthermore, the California law applies only to companies "that [collect] personally identifiable information through the Internet about individual consumers";[83] other forms of data compilation and profiling are not covered. Thus, although this requirement is moderately satisfied in theory, in practice it is not.

There must be a way for an individual to find out what information about him is in a record and how it is used. It is less clear that this requirement is satisfied, even in theory. Even California's online privacy law does not require that companies make such information available; rather, they must disclose if they do.[84] Again, though, even if all companies make such information available, it is infeasible for consumers to request changes to a record they do not know exists.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There is no way for individuals to understand how their data is used. Much of it, of course, is used for advertising, but that covers a wide range of activities. Facebook has been accused of deliberate vagueness about how it establishes connections between people[85] and of using information collected for two-factor authentication, a security feature, for targeting ads.[86] The risk of information leakage from targeted ads has even reached popular culture.[87]

The existence of partners muddies the issue even further. The most obvious case in point is the information that Cambridge Analytica obtained from Facebook.[88] Facebook "routinely allows researchers to have access to user data for academic purposes—and users consent to this access when they create a Facebook account."[89] Arguably, someone did violate agreements, since the researcher who originally obtained the data appears to have been barred from further redistribution.[90] From a privacy perspective, though, users consented to the original transfer and then lost control of their data.

[78] Solove and Hartzog, *supra* note 72, at 639.

[79] *Id.* at note 48.

[80] Shirey, *supra* note 17.

[81] Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 13.

[82] Online Privacy Protection Act, Cal. Bus. & Prof. Code §§22575-22579 (2004).

[83] Cal. Bus. & Prof. Code §22575(a).

[84] Cal. Bus. & Prof. Code §22575(b)(2).

[85] Kashmir Hill. "How Facebook Figures Out Everyone You've Ever Met". In: *Gizmodo* (Nov. 7, 2017). URL: https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691.

[86] Kashmir Hill. "Facebook Is Giving Advertisers Access to Your Shadow Contact Information". In: *Gizmodo* (Sept. 26, 2018). URL: https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051.

[87] *Kevin and Kell*, Oct. 12, 2018, https://www.kevinandkell.com/2018/kk1012.html.

[88] Kevin Granville. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens". In: *New York Times* (Mar. 19, 2018). URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[89] *Id.*

[90] *Id.*

There must be a way for an individual to correct or amend a record of identifiable information about him. As with the second point, though it may be true in theory, in practice people are unaware of where their data is stored and hence of how it may be corrected. Furthermore, there are so many data collectors that attempting to correct all erroneous records would be extremely time-consuming—and one never knows when the next data collector will spring up.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. As we have seen, even the best Internet companies, *e.g.*, Facebook, are vulnerable to technical security failures. No security paradigm should be based on the assumption that large collections of data can be protected.

The FIPPs, then, and by extension the whole concept of notice and consent, no longer fit the modern world. Many collectors are effectively unknown; there are also technical means of data collection that are opaque even to technically sophisticated users. Furthermore, the same data and databases are used to both answer user requests and to invade privacy. Our ability to consent has vanished.

IV Use Restrictions as a Way Forward

In contrast to notice and consent, some, most notably President Obama's Council of Advisors on Science and Technology, have advocated use restrictions.[91] That is, instead of asking individuals to consent to the collection of their data, they are asked to consent to how it is used.

Landau gives several specific examples of where use restrictions are employed today.[92] She notes that a National Academies study committee[93] concluded that the only way to control bulk signal intelligence collection is to restrict how the data is actually used. Other examples she gives, *e.g.*, the Shibboleth information-sharing system, are examples of "attribute credentials".[94] Attribute credentials, as opposed to the more common identity credentials, say what you're allowed to do rather than who you are. They are thus (generally) privacy-preserving. The easiest analogy is cash versus a line of credit: the former lets you buy things; the latter does, too, but based on who you are; it is therefore not privacy-preserving.

In many ways, this is an attractive idea. However, the details are extremely important. Note the careful wording of the PCAST report's first recommendation: 'Policy attention should focus more on the actual uses of big data and less on its collection and analysis."[95] The group did not recommend any particular mechanism based on use restriction, and in particular said nothing about how consent should be given and by whom; rather, they suggested it as a policy direction. In other words, they recommend that policymakers consider it, but do not suggest any way in which it can be accomplished.

It turns out that there are a number of problems with trying to employ use restrictions in a broader commercial sense, and in particular in trying to craft regulations to instantiate them as an alternative to notice and consent. The first is defining what a "use" is. Is each advertising campaign a new use? Assuredly not. Online advertising versus door-to-door sales? That's a closer call; most people would view the latter as far more intrusive. A natural answer is to define categories of uses, but that isn't easy, either. Would-be data abusers would naturally prefer broad, inclusive categories; privacy-sensitive individuals would prefer narrow ones. But who should define the categories, and how? How would they be updated over time?

A second important question is who should grant consent for a specific use. Having a government data protection agency do so is more compatible with European approaches to privacy; it may not pass muster in the U.S. The obvious answer, individual consent, is problematic: how are the individuals to be located? Data collected long ago can still be valuable, see, *e.g.*, a study on Alzheimer's incidence today correlated with results from a 1960 aptitude test.[96] Locating

[91] PCAST, *supra* note 33.

[92] Susan Landau. "Control use of data to protect privacy". In: *Science* 347 (Jan. 30, 2015), pp. 504–506. DOI: 10.1126/science.aaa4961.

[93] National Research Council. *Bulk Collection of Signals Intelligence*. Washington, DC: National Academies Press, 2015. URL: http://nap.edu/19414.

[94] For a different example of attribute credentials, see Carl Ellison et al. *SPKI Certificate Theory*. RFC 2693. Sept. 1999. URL: http://www.rfc-editor.org/rfc/rfc2693.txt.

[95] PCAST, *supra* note 33, at 49.

[96] Alison Huang, Kiersten L. Strombotne, Elizabeth Mokyr Horner, and Susan J. Lapham. "Adolescent cognitive aptitudes and later-in-life Alzheimer disease and related disorders". In: *JAMA Network Open* 1.5 (2018), e181726–. DOI: 10.1001/jamanetworkopen.2018.1726.

the test subjects was problematic; the researchers only found 38% of the test-takers,[97] and were able to achieve that much only because they were able to tap into high school 50th reunion data.[98] Nor did the researchers seek individual consent; they instead obtained a waiver from their institutional review board,[99] a solution more applicable to academic research than to industry efforts.

Furthermore, and as noted, many privacy violations occur independent of the existence of any PII. Consent to assorted categories could, presumably, be set at collection time, perhaps by drawing on browser or device defaults, but there would be no way to change such consent in the future, whether for new uses, new abuses, or changed personal preferences. Auditing compliance with user restrictions is also a problem.

The third problem is the potential for later misuse of collected data. It is a truism in the privacy community that the most serious abuses happen when data collected for one purpose is then used for another. Serious abuses have happened, *e.g.*, the misuse of census data to intern Japanese Americans during World War II.[100] There is the additional risk of hacking.[101] Data that does not exist cannot be abused.

Finally, and perhaps fatally for proposals to enact statutory restrictions on data use, there is a First Amendment issue. The Supreme Court has held that "An individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated."[102] If data is legally collected—that is, if we abandon notice and consent—that ruling would appear to doom any mandatory limits on how that data is used. A solution would thus have to turn on conditional consent: a user might voluntarily turn over data only to entities that promised to abide by certain restrictions. Violating that promise would presumably be seen as unfair and deceptive by the FTC.

Use controls do seem to avoid the insoluble problems of collection limits and notice and consent. An approach based on categories with user consent to selected categories, either at time of collection or later, might be feasible if embedded in a suitable legal framework.

V Recommendations

I recommend that the following steps be adopted.

- First and foremost, we need a new paradigm for privacy, one that goes beyond notice and consent. One can hearken back to Warren and Brandeis' definition, "the right to be let alone";[103] however, that is not an operational definition in the same sense as the more modern ones: it does not tell us what rules or restricions should be imposed. This is a research question. As noted, PCAST[104] and Landau[105] have proposed use restrictions. Waldman suggests an approach to privacy by design based on liability law;[106] he notes, though, that he is "not suggesting a new products liability tort for privacy-invasive design through which individuals could sue

eprint: /data/journals/jamanetworkopen/937489/huang_2018_oi_180105.pdf. URL: +%20http://dx.doi.org/10.1001/jamanetworkopen.2018.1726.

[97] Huang, Strombotne, Horner, and Lapham, *supra* note 96, at 2.

[98] Tara Bahrampour. "In 1960, about a half-million teens took a test. Now it could predict the risk of Alzheimer's disease." In: *Washington Post* (Sept. 21, 2018). URL: https://www.washingtonpost.com/local/social-issues/in-1960-about-half-a-million-teens-took-a-test-now-it-could-predict-whether-they-get-alzheimers/2018/09/20/fcbabebe-b864-11e8-a7b5-adaaa5b2a57f_story.html.

[99] Huang, Strombotne, Horner, and Lapham, *supra* note 96, at 2.

[100] Lori Aratani. "Secret use of census info helped send Japanese Americans to internment camps in WWII". in: *Washington Post* (Apr. 6, 2018). URL: https://www.washingtonpost.com/news/retropolis/wp/2018/04/03/secret-use-of-census-info-helped-send-japanese-americans-to-internment-camps-in-wwii/.

[101] Getting illicit access to vast troves of personal data does not require the skills of a national intelligence agency. Even amateurs have been able to do it; *see*, *e.g.*, Thomas Brewster. "How An Amateur Rap Crew Stole Surveillance Tech That Tracks Almost Every American". In: *Forbes* (2018). URL: https://www.forbes.com/sites/thomasbrewster/2018/10/12/how-an-amateur-rap-crew-stole-surveillance-tech-that-tracks-almost-every-american/.

[102] Sorrell v. IMS Health Inc., 564 U.S. 552, 568 (U.S. June 23, 2011).

[103] Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy". In: *Harvard Law Review* 4.5 (Dec. 1890). URL: https://www.jstor.org/stable/1321160, at 195.

[104] PCAST, *supra* note 33.

[105] Landau, *supra* note 92.

[106] Ari Ezra Waldman. "Privacy's Law of Design". In: *UC Irvine Law Review* (Oct. 8, 2018). Draft. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263000.

technology companies and data collectors."[107] Other scholars have suggested privacy torts.[108] I suggest that the first step would be a study by the National Academies of Science, Engineering, and Medicine; the charge to such a study committee would to identify existing proposals, to evaluate their advantages, disadvantages, and feasibility, and to define the parameters of future projects aimed at crafting a new paradigm.

- We need a more modern definition of "injury". Limiting it to direct financial harm, *e.g.*, through theft of credit card numbers, or to disclosure of health information, is inadequate. For example, simple disclosure of group membership can be very dangerous. In one incident, confusion over Facebook's privacy policies led to some students being outed as gay to their parents, with devastating effects on their family ties.[109] Even for those who advocate less regulation, more clarity here would be useful; it would lend more predictability to the FTC's enforcement actions.[110]

- The authority of the Federal Trade Commission to act against security and privacy breaches should be enhanced by statute. Today, "[T]he FTC lacks the general authority to issue civil penalties and rarely fines companies for privacy-related violations under privacy-related statutes or rules that provide for civil penalties... When the FTC does include fines, they are often quite small in relation to the gravity of the violations and the overall net profit of the violators. This is because any fines issued by the FTC must reflect the amount of consumer loss."[111]

- Barring a new paradigm, use controls seem to be a promising approach, assuming that the constitutional issues can be resolved. Defining categories and consent mechanisms[112] is an open question, though arguably less daunting than a completely new paradigm. A study committee, possibly under the auspices of the FTC, should define a set of categories; data users would assign their effort to a particular category.[113] Misassignment or misleading users would be a deceptive practice, per the Federal Trade Commission Act.[114] It is crucial that user permissions be independent of each site. That is, what is protected is the data, not the source from which it came; to do otherwise is to fall back into the same traps as today's notice and consent. Someone who wished to opt out of, say, email marketing pitches should only have to do it once, or at most once per email address used. This might require a central registry of preferences, but we already use such for the "Do Not Call" list.[115]

- Once a new paradigm is selected, be it use restrictions or something else, privacy policies based on notice and consent should be phased out as swiftly as is feasible. Although the GDPR may still require it, many web sites have dual policies already, to comply with the GDPR when they must but to take advantage of looser American regulations when they can.

- Finally, if we have to stick with notice and consent, two major changes should be made. First, it should be mandatory to disclose privacy practices in a simple, standardized format, akin to nutrition labels on food. Research suggests that this approach is very promising.[116] Second, site operators' privacy policies must disclose the policies used by any embedded sites. The site operator can, at least in principle, control this; the user cannot.

[107] Waldman, *supra* note 106, at 8.

[108] *Id.* at note 22.

[109] Geoffrey A. Fowler. "Watched: When the Most Personal Secrets Get Outed on Facebook". In: *Wall Street Journal* (Oct. 13, 2012). URL: https://www.wsj.com/articles/SB10000872396390444165804578008740578200224 ("The two students were casualties of a privacy loophole on Facebook—the fact that anyone can be added to a group by a friend without their approval. As a result, the two lost control over their secrets, even though both were sophisticated users who had attempted to use Facebook's privacy settings to shield some of their activities from their parents.").

[110] The FTC is looking into the question (*see* Federal Trade Commission. *FTC Informational Injury Workshop*. Oct. 2018. URL: https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018.pdf) but there is no consensus.

[111] Solove and Hartzog, *supra* note 72, at 605.

[112] *See* Section IV, *supra*.

[113] Ironically, there is the potential for privacy violations from this very practice intended to preserve privacy. Suppose there are 24 different use categories. That means there are 2^{24} (about 16 million) different combinations of settings. Unusual-enough choices would themselves constitute a tracking mechanism.

[114] 15 U.S.C. §45.

[115] 16 C.F.R. §310.4(b)(iii)(B).

[116] *See, e.g.,* Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '10. Atlanta, Georgia, USA: ACM, 2010, pp. 1573–1582. ISBN: 978-1-60558-929-9. DOI: 10.1145/1753326.1753561. URL: http://doi.acm.org/10.1145/

Note that these two notions are linked: a simple-to-read privacy policy can easily be encoded in machine-readable form and passed in that form to advertisers; they would have to comply with it.

The most important thing, though, is to act and to act now. Every day, more data is collected; every day, more abuses and leaks take place.

Acknowledgments

I would like to thank Joseph Lorenzo Hall, Susan Landau, Joel Reidenberg, and David Vladeck for their many helpful comments on this document. The opinions expressed here, however, are mine.

1753326.1753561 and Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. "A "Nutrition Label" for Privacy". In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. SOUPS '09. Mountain View, California, USA: ACM, 2009, 4:1–4:12. ISBN: 978-1-60558-736-3. DOI: 10.1145/1572532.1572538. URL: http://doi.acm.org/10.1145/1572532.1572538.