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

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

Comments of Privacy Law Scholars

via e-mail to privacyrfc2018@ntia.doc.gov
November 9, 2018

Samuelson-Glushko Technology Law & Policy Clinic (TLPC) • Colorado Law

Nathan Bartell
Elliott Browning
Zachary DeFelice
Student Attorneys

Prof. Blake E. Reid
Director

blake.reid@colorado.edu • 303.492.0548

Affiliations listed for identification only

Mark Bartholomew
Professor of Law
University at Buffalo School of Law

Steven M. Bellovin
Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University
Affiliate Faculty, Columbia Law School
Visiting Scholar, Center for Law and Information Policy, Fordham University School of Law

Sebastian Benthall
Research Scholar
Information Law Institute
New York University School of Law

Jordan M. Blanke
Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law
Stetson School of Business & Economics, Mercer University
External Affiliate, Indiana University Bloomington, Ostrom Workshop in Data Management & Information Governance, and Cybersecurity & Internet Governance

Kiel Brennan-Marquez
Associate Professor & William T. Golden Research Scholar
University of Connecticut School of Law

Danielle K. Citron
Morton & Sophia Macht Professor of Law
University of Maryland Francis King Carey School of Law

Roger Allan Ford
Associate Professor of Law and Franklin Pierce Faculty Fellow, University of New Hampshire School of Law
Visiting Fellow, Information Society Project at Yale Law School

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University School of Law

Meg L. Jones
Assistant Professor of Communication, Culture & Technology
Georgetown University

Margot E. Kaminski
Associate Professor of Law,
University of Colorado Law School
Privacy Director, Silicon Flatirons Center
Affiliated Fellow, Information Society Project at Yale Law School

Karen Levy
Assistant Professor
Department of Information Science
Associated Faculty Cornell Law School

Art Neill
Clinical Professor
California Western School of Law
Executive Director, New Media Rights

Helen Nissenbaum
Professor of Information Science
Cornell Tech

Paul Ohm
Professor of Law
Georgetown University Law Center

Frank Pasquale
Professor of Law
University of Maryland Francis King Carey School of Law

Summary

While we appreciate the NTIA's sincere efforts to shift away from protecting data privacy through a largely ineffective notice-and-choice regime, we worry that the proposed contextual risk-management approach to privacy equally risks affording inadequate protection for consumers in practice.

Our primary aim in submitting this comment is to provide NTIA with a more complete set of data privacy principles and with detailed examples of how principles have been made more effective in practice.

NTIA's RFC has three critical problems:

1. It misses a number of centrally important concepts, principles, and trends in data privacy law;
2. It proposes high-level principles of such breadth that they risk being implemented in ways that fail to protect consumers; and
3. It frames harmonization in a way that neglects to take into account both historic state interests in protecting privacy, and the international context of upward harmonization with the EU's General Data Protection Regulation (GDPR).

Accordingly, we begin by discussing several centrally important concepts, principles, and trends in data privacy law that were not considered in the Request for Comments (RFC):

- Privacy as a fundamental individual right;
- Privacy as contextual integrity;
- Privacy and manipulation;
- Purpose specification;
- Privacy by design; and
- The expanding definition of personally identifiable information

Next, we discuss ways in which the RFC's proposed privacy principles can be implemented effectively and provide multiple examples from both United States and international law.

Finally, we address NTIA's high-level goals of FTC enforcement and regulatory harmonization.

Table of Contents

Discussion

The above-listed privacy law scholars respectfully comment on NTIA's Request for Comments (RFC) in the above-referenced docket.[1] We research, write, and teach in the areas of privacy, data protection, and data security law.

At this historic moment for data privacy, NTIA can guide the United States into a future of data practices that addresses increasing concerns about privacy and autonomy, and respects individuals' rights. A strong federal approach to data privacy would not only encourage individuals to trust and participate in the digital economy and on digital platforms, but could enable U.S. companies to gain a more competitive position abroad.

Individuals, courts, and policymakers in this country and around the world have shown a growing appetite for effective data privacy law. This year has seen the enactment of the California Consumer Privacy Act (CCPA), the implementation of the General Data Protection Regulation (GDPR) in the European Union and similar laws abroad, and the Supreme Court's important decision in *Carpenter v. United States*.[2] These recent developments indicate widespread and cross-cultural concerns about data practices, and show both fast-developing understandings of what constitutes data privacy harm and a growing consensus about what measures should be taken to prevent it.

The RFC envisions NTIA's policy as based on a foundation of consumer trust and built on risk management. However, the RFC has several significant flaws:

- The RFC misses several important concepts, principles, and trends in data privacy law, including contextual integrity, the problem of manipulation, privacy by design, and an expanding definition of personal information.
- The RFC's proposed high-level principles risk being implemented without sufficiently protecting consumer privacy.
- The RFC's framing of harmonization neglects to take into account both historic state interests in protecting privacy, and the international context of upward harmonization with the GDPR.

We address each of these shortcomings in turn. First, we address concepts, principles, and trends that are missing from the RFC. Second, we detail how the proposed Privacy Outcomes might be implemented in effective, protective ways with references to both existing U.S. law

---

[1] *Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC"), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

[2] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West) ("CCPA"); Council Regulation (EU) 2016/679, OJ L 119/1 ("General Data Protection Regulation" or "GDPR"); Lei No. 13,709 de 14 de Agosto, Diário Oficial da União [D.O.U.] de 15.08.18 (Braz.) ("*Lei Geral de Proteção de Dados Pessoais*" or "LGPD"); Carpenter v. United States, 138 S. Ct. 2206 (2018).

and international practices. Finally, we address two of the RFC's Goals—Federal Trade Commission (FTC) enforcement and the issue of harmonization, both within the United States and internationally.

I. Missing Concepts, Principles, and Trends in Privacy Law

While we support the idea of re-focusing consumer privacy away from notice-and-choice, the RFC neglects to address several concepts, principles, and recent trends that are central to data privacy protection. Missing concepts include:

- Privacy as a fundamental individual right;
- Privacy as contextual integrity;
- The connection between privacy and fairness; and
- The connection between privacy and manipulation.

Missing principles—by which we refer to the foundations and elements of data protection laws around the world—include the principles of:

- Purpose specification and related use limitations;
- Data quality;
- Collection limitation; and
- Privacy by design.

Missing trends—by which we mean significant recent developments in lawmaking around the world—include:

- Expanding the definition of personal information;
- Recognizing privacy in public spaces;
- Recognizing the kinds of privacy problems created by "big data"; and
- Extending privacy rules to cover third parties such as data brokers.

A. Missing Concepts

We begin with missing concepts. The RFC largely characterizes data privacy as an issue of consumer trust in the companies with which they are directly interacting as consumers.[3] While this is a potentially useful and central conceptualization of privacy, and one on which FTC enforcement has largely been based, focusing on consumer trust alone can omit other characterizations of privacy that can lead to different, sometimes broader, understandings of privacy harms.

[3] RFC, 83 Fed. Reg. 48,600.

i. Privacy as a Fundamental Individual Right

In the European Union, privacy and data protection are recognized as fundamental individual rights, even against private actors.[4] While in the United States we think of the Constitutional right to privacy under the Fourth Amendment as giving protection only against the government, we in fact have many privacy regimes that give individuals rights against the private sector.[5] The Supreme Court has recently recognized that privacy protections are intimately entwined with other well-recognized individual rights: for example, to free speech and freedom of association.[6]

The enactment of both federal and state privacy laws in the United States shows that individuals understand the close links between privacy and individual autonomy, and between privacy and other individual rights, from freedom of expression to due process to autonomy in the marketplace. Even when companies are not state actors, their actions can cause harms that not only violate consumer trust but fundamentally affect individuals' ability to control and shape both their digital and real-world selves. This connection between privacy and the ability to shape one's self has been referred to in many ways: as autonomy, as control, as dignity, as "boundary management," as "play," and as the use of "obscurity," both digital and physical, to manage disclosure.[7]

---

[4] Charter of Fundamental Rights of the EU, Arts. 7 (Respect for private and family life), 8 (Protection of personal data), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT; *see, e.g.*, Digital Rights Ireland v. Minister for Communications (April 8, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293. For an example of the application of fundamental rights against companies—i.e., "horizontal" effects—see Case C-144/04, Mangold v. Helm, 2005 Eur. Ct. H.R. 709 (Nov. 22, 2005), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004CJ0144; *see also* Paul Schwartz & Karl-Nicolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEORGETOWN L. J. 121, 126 (2017), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3913&context=facpubs.

[5] Fair Credit Reporting Act, 15 U.S.C. ch. 41, subch. III ("FCRA"); Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat 1936 (1996) ("HIPAA"); Video Privacy Protection Act, 18 U.S.C. § 2710 ("VPPA"); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505 ("COPPA").

[6] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J. concurring) (discussing "familial, political, professional, religious, and sexual associations"). This has caused the Court to weigh First Amendment interests on both sides in evaluating First Amendment challenges to privacy laws governing the private sector. *See, e.g.* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001).

[7] Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1907-1932 (2013), https://harvardlawreview.org/2013/05/what-privacy-is-for/(discussing the tendency of American scholars to characterize privacy as autonomy, and referring to privacy as "boundary management" and "the play of everyday practice"*)*; Woodrow Hartzog & Frederic D. Stutzman*, The Case for Online Obscurity* (February 23, 2012). 101 CAL. L. REV. 1 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597745; Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1132-35 (2015) (building on the work of social psychologist

Conceptualizing privacy as consumer trust, narrowly defined, has an important practical implication: it focuses regulation on the relationship between individuals and the particular companies with which they interact.[8] By contrast, conceptualizing privacy as an individual "right" impacting individual autonomy suggests extending protection to follow personal data. Consumer trust, narrowly defined (and as contrasted with broader understandings of trust[9]) may capture only one aspect of the privacy concerns raised by the following scenarios:

- A job applicant whose potential employer decides not to hire her after discovering the applicant's health status from a digital profile may be concerned about a breach of trust by her health providers or websites she has visited. But she is also concerned about the flow of personal information from a third-party profiler, with which the applicant likely has never interacted as a consumer, to the potential employer.
- A person whose family or community has decided to reject him after discovering his online reading habits has experienced a breach of trust by the websites he visits. But he also worries about his ability to read what he wants without changing how others perceive him, and the outcomes of unwanted personal data flow.[10]
- An online consumer who consistently receives advertisements offering him higher priced goods or worse terms on a loan based on information about his cell phone's operating system has experienced a breach of trust by his cell phone provider or by websites that collect that information. But he also worries about misuse of his data, discrimination, and his autonomy in the marketplace.[11]

Irwin Altman in defining privacy in physical spaces); Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1689-1720 (2017) (explaining that efforts to maintain privacy can be a form of outward expression).

[8] *See* Roger Allan Ford, *Unilateral Invasions of Privacy*, 91 Notre Dame L. Rev. 1075 (2016).

[9] Exemplary articulations of the broader versions of the trust include Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* 49-76 (2018) and Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 447-456 (2016). Trust can be conceptualized as a resource of social capital between two or more parties concerning the expectations that others will behave according to accepted norms. It is the favorable expectations regarding other people's actions and intentions, or the belief that others will behave in a predictable manner. Trust includes a willingness to accept some risk and vulnerability toward others and allows us to engage, in person and online, in the absence of perfect knowledge.

[10] Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 216-19 (2015) (highlighting that unwanted disclosure of personal information can lead to downstream social harms, including discrimination).

[11] Leonid Bershidsky, *Own an Android Phone? You Might Not Get That Loan,* Bloomberg Opinion, (May 4, 2018), https://www.bloomberg.com/opinion/articles/2018-05-04/algorithms-and-data-could-determine-creditworthiness; Davey Alba, *Online Stores Change Prices Depending on How You Shop. Here's How.,* WIRED (Nov. 13, 2014), https://www.wired.com/2014/11/online-price-discrimination/.

- A person who sees a drone fly over her fenced backyard is concerned not about her trust in the drone operator but about her ability to control access to her family and home environment and relax in the privacy of her home.[12]

This is not to suggest that consumer trust, or trust writ more broadly, is a poor framework for privacy. Trust is the basis for privacy laws around the world, invokes complex contextual understandings of privacy, and can trigger robust fiduciary-like protections.[13] But consumer trust, narrowly defined, should work together with the full spectrum of data privacy harms to underpin the full spectrum of regulatory approaches that we now see in both U.S. laws and laws around the world.[14]

ii. Privacy as Contextual Integrity

Another concept of privacy missing from the RFC is the idea of privacy as "contextual integrity."[15] While the RFC refers several times to context, it does so largely while explaining that context should be taken into account when evaluating how much—or how little—privacy protection to provide.[16] Contextual integrity, by contrast, counsels awareness of situational norms and information flows. It suggests connecting data use to individual expectations at the time data is shared. The absence of contextual integrity in the RFC is striking, given the centrality of the concept to both recent consumer privacy proposals and recent FTC practices.[17]

---

[12] Margot E. Kaminski, *Regulating Real-World Surveillance*. 90 WASH. L. REV. 1113, 1136 (2015), https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1483/90WLR1113.pdf?sequence=1&isAllowed=y.

[13] Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. 1183, 1205 (2016), https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.; Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For,* Harvard Business Review (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for.); Neil M. Richards and Woodrow Hartzog, *Taking Trust Seriously in Privacy Law,* 19 STAN. TECH. L. REV. 431 (2016), https://ssrn.com/abstract=2655719; Neil M. Richards and Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEORGETOWN L. J., 123 (2007), https://ssrn.com/abstract=969495; Ari Ezra Waldman, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (Cambridge University Press, 2018).

[14] Daniel J. Solove, UNDERSTANDING PRIVACY (Harvard University Press, 2008).

[15] Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford University Press, 2010).

[16] RFC, 83 Fed. Reg. at 48,601 ("Using a risk-based approach, the collection, use, storage, and sharing of personal data should be reasonable and appropriate to the context").

[17] Lesley Fair, *Letters to App Developers Caution Against Info Surprises,* FTC Business Blog (Mar. 17, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/03/letters-app-developers-caution-against-info-surprises.; Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy,* THE ATLANTIC (Mar. 29, 2012),

Contextual integrity both connects to and expands beyond an understanding of privacy as consumer trust. Individuals often reveal information in the context of a trusted relationship, or within a particular physical or social setting. Those settings, both social and physical, contain within them internalized norms of information use. Individuals then expect that the information will not pop up in other contexts: they expect "no surprises."[18] A privacy violation occurs when information a person has disclosed in one context appears, unexpectedly, in another.

Contextual integrity provides a backstop for data privacy practices by urging that companies tailor behavior to avoid surprising individuals with the use of information outside of the context in which it was originally obtained. It thus ties in to the foundational data privacy principle of "purpose specification," which is also missing from the RFC.[19]

By way of real-world examples,[20] a person may disclose health information to a health-related website, behave a particular way in the privacy of the home, or reveal information to stores through shopping habits. If that health information then appears in a targeted online advertisement,[21] home behavior is sent to an insurance company,[22] or shopping patterns are mined to reveal personal health information to a family member,[23] then contextual integrity is violated and a privacy harm occurs.

---

https://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/.

[18] *See, e.g.,* MOZILLA, *Data Privacy Principles*, https://www.mozilla.org/en-US/privacy/principles/; *see also* Article 29 Working Party, GUIDELINES ON TRANSPARENCY UNDER REGULATION 2016/679, at 7 ("the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should *not be taken by surprise* at a later point about the ways in which their personal data has been used") (emphasis added).

[19] *See* discussion *infra*, Part I.B.iii.

[20] *See* Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018), (Google tracks your movements even if users set the settings to prevent); *see also* Emily Glazer et al, *Facebook to Banks: Give Us Your Data, We'll Give You Our Users*, WALL STREET JOUR. (Aug. 6, 2018) (Facebook asked large U.S. banks to share financial information on their customers).

[21] *See, e.g.,* Stephanie Daigle, *Here's Looking at You: Targeting Tips for Facebook,* INFLUENCE HEALTH BLOG (Feb. 1, 2018), https://www.influencehealth.com/blog/heres-looking-at-you-targeting-tips-for-facebook ("For example, we can target adults who have liked The American Heart Association; maybe they would be likely to interact with a cardiology ad. We would also want to target other interests, like hypertension awareness or heart disease awareness").

[22] Ed Leefeldt, *How Amazon's Echo Lets Businesses Into Your Home,* CBS MONEY WATCH (March 8, 2017, 6:00 AM), https://www.cbsnews.com/news/how-amazons-echo-lets-businesses-into-your-home/.

[23] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did,* FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#12c153306668.

iii. Privacy and Fairness

The absence of fairness in the RFC is also a remarkable omission. Fairness is one of the foundational principles of the EU's GDPR, and is so central to data privacy policy that it is included in the title of the Fair Information Practice Principles (FIPPs) on which data privacy laws around the world are built.[24] The FTC's recent Big Data Report and related scholarship connect data privacy practices to both outright discrimination and to more procedural understandings of fairness, including concerns about individual due process.[25]

Big data analytics and the use of machine-learning-based decision-making can raise concerns about both accidental and deliberate discrimination.[26] How data are collected and labeled can give rise to unintentionally discriminatory outcomes.[27] In one example recently noted by the FTC, the city of Boston created a smartphone application to report road conditions to the city.[28] Reliance on input from this application would have skewed road repair services towards higher income neighborhoods whose residents had smartphones and downloaded the app. The FTC noted: "This example demonstrates why it is important to consider… issues of underrepresentation and overrepresentation in data inputs before launching a product or service in order to avoid skewed and potentially unfair ramifications."[29]

Unfairness can also enter a system when a computer program is designed to focus on or give weight to factors that unintentionally discriminate. For example, evaluating whether a job applicant is likely to be late to work by looking at the proximity of their home to the job can

---

[24] GDPR art. 5(1)(a) ("Personal data shall be…processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')").

[25] *See e.g.*, Federal Trade Commission, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.; Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016), http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.; Danielle Keats Citron, *Technological Due Process,* 85 WASH. U. L. REV. 1249 (2008), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview; Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions,* 89 WASH. U. L. REV 1 (2014), https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1318/89wlr0001.pdf?sequence=1.

[26] Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016), http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.

[27] Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 708 (2016), http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.

[28] Federal Trade Commission, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016) at 27, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; see also https://hbr.org/2013/04/the-hidden-biases-in-big-data, which brought this example to the FTC's attention.

[29] *Id.*

bias a job search against applicants with lower incomes or from particular communities.[30] Discrimination can also occur through what is known as "redundant encoding," where a variable that seems neutral—like a zip code—in fact encodes for characteristics that we ordinarily think of as impermissible bases for a decision, like race.[31] Finally, data analytics can hide intentional discrimination, allowing companies to treat consumers differently based on race, gender, sexual orientation, or political preferences.[32]

Fairness concerns also take the form of concerns about due process.[33] The FIPPs referenced in the RFC are founded on the understanding that there can be great power imbalances between individuals and the entities that hold and process data about them.[34] Accordingly, the FIPPs are geared at restoring some power to individuals over the course of the data lifecycle, as information is collected, processed, maintained, stored, and used. Shifting to a risk-management approach to data practices threatens to undermine these individual procedural rights. A shift towards risk-management should be careful not to disempower individuals by giving companies the discretion to decide when to afford individuals process rights.

iv. Privacy and Manipulation

The RFC does not acknowledge or discuss that surveilling consumers allows companies to manipulate them.[35] Surveillance creates power imbalances, not just because knowledge is

---

[30] Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 714 (2016), http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.

[31] Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 692 (2016), http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.

[32] Brakkton Booker, *HUD Hits Facebook For Allowing Housing Discrimination,* NPR (Aug. 19, 2018), https://www.npr.org/2018/08/19/640002304/hud-hits-facebook-for-allowing-housing-discrimination.

[33] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. U. L. REV 1 (2014),https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1318/89wlr0001.pdf?sequence=1.; Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms,* 55 B.C.L. REV. 93 (2014), https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr.

[34] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy,* 2001 STAN. TECH. L. REV. 1, https://heinonline.org/HOL/LandingPage?handle=hein.journals/stantlr2001&div=2&id=&page=; U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS 29-30, 41-42 (1973) ("HEW Report") ("Even in non-governmental settings, an individual's control over the personal information that he gives to an organization or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused.").

[35] *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, GEORGE WASH. L. REV. 82 (2014); Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. OF PA. L. REV. 1311 (2015); Mark Bartholomew, ADCREEP: THE CASE AGAINST MODERN

power, but because information can be used to nudge consumers towards particular behavior without their knowledge.[36] When companies know far more about their consumers than they disclose, this imbalance enables companies not only to take advantage of information asymmetries, but to exploit predictable human behavior.[37]

There has been increased attention in recent years to the close connection between surveillance and manipulation. "The idea that technology can be used to persuade people and change their behavior isn't a crackpot theory; it's an entire industry supported by established research on human vulnerability."[38] A number of scholars now call for attention to consumer manipulation as a particularly important type of data privacy harm.[39] This behavior has been referred to as "digital market manipulation," with scholars predicting that a "set of emerging technologies and techniques will empower corporations to discover and exploit the limits of each individual consumer's ability to pursue his or her own self-interest."[40]

For example, a firm might change its targeted advertisements in real time—known as persuasion profiling—to prey on a consumer's specific vulnerabilities.[41] Research suggests that some consumers are motivated by wanting to do what others do, while others respond to a desire for exclusivity or a fear of missing out. Thus companies might label a product "best-selling" to convince followers, while suggesting product scarcity to those motivated by exclusivity.[42] More nefarious examples of preying on user vulnerabilities include targeting advertisements for, say, gambling towards people with known gambling addictions.[43] Interfaces can be designed, too, to manipulate individuals and exploit behavioral tendencies,

---

MARKETING 63-85 (Stanford University Press, 2017); Brett Frischmann & Evan Selinger, RE-ENGINEERING HUMANITY 35-42 (Cambridge University Press, 2018).

[36] *Id.*

[37] *See* Daniel Kahneman, THINKING FAST AND SLOW (2011); Dan Ariely, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2008); DANIEL GILBERT, STUMBLING UPON HAPPINESS (2006).

[38] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018) at 142.

[39] *Id.* at 145 ("[P]rivacy law should be concerned about designs that . . . take unreasonable advantage of people's understanding, limited abilities, or reliance on relationships . . . . [P]rivacy law should ask whether a particular design interferes with our understanding of risks or exploits our vulnerabilities in unreasonable ways"); *see* Roger Allen Ford, *Data Scams*, (Nov. 8, 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281460.

[40] Calo, *supra* n. 35 at 999 ("Firms will increasingly be able to trigger irrationality or vulnerability in consumers").

[41] *Id.* at 1017; Hartzog, *supra* note 38 at 146.

[42] Calo, *supra* n. 35 at 1017.

[43] Mattha Busby, *Revealed: how gambling industry targets poor people and ex-gamblers*, THE GUARDIAN (Aug. 31, 2017, 1:31 PM), https://www.theguardian.com/society/2017/aug/31/gambling-industry-third-party-companies-online-casinos.

from pop-up ads designed to trick users into clicking on them to unnecessary forms or blinking advertisements designed to distract.[44]

Platforms are well aware of their capacity to manipulate and exploit users. In 2014, Facebook set off a storm of controversy by publishing an experiment on almost 700,000 users evaluating "emotional contagion"—that is, how users react to negative and positive content conveyed through a social network.[45] The study found that users' emotions can be manipulated by controlling the content to which they are exposed.

The idea that powerful firms can manipulate unknowing individuals based on access to and analysis of personal data is one of the core concerns motivating, for example, the California Consumer Privacy Act, which was enacted in response to the Cambridge Analytica scandal.[46] Similarly, GDPR Guidelines suggest that targeted advertising should be subject to more stringent regulatory requirements when companies "us[e] knowledge of the vulnerabilities of the data subjects targeted" or deliver an advertisement in a particularly manipulative way.[47] The connection between surveillance and manipulation has long been part of the conversation about marketing directed at children, with advertisers recognizing as early as 2000 that children are vulnerable to manipulation through incentives like games or prizes.[48]

---

[44] Hartzog, *supra* note 38 at 147-148; *see also* Gregory Conti and Edward Sobiesk, "Malicious Interface Design: Exploiting the User 271," paper presented at WWW 2010: The 19th International World Wide Web Conference, Raleigh, NC, April 26–30, 2010, http://www.Rumint.org/gregconti/publications/201004malchi.pdf; Gregory Conti and Edward Sobiesk, "Malicious Interfaces and Personalization's Uninviting Future," IEEE SECURITY AND PRIVACY 7, 73 (2009), http://www.rumint.org/gregconti/publications/j3pri.pdf.

[45] Katy Waldman, *Facebook's Unethical Experiment*, SLATE (June 28, 2014, 5:50 PM), https://slate.com/technology/2014/06/facebook-unethical-experiment-it-made-news-feeds-happier-or-sadder-to-manipulate-peoples-emotions.html; Adam D.I. Kramer et al., *Experimental evidence of massive-scale emotional contagion through social networks*, 111 PNAS 24 (June 17, 2014), http://www.pnas.org/content/pnas/111/24/8788.full.pdf; James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*, 220 COLO. TECH. J. 13 (2015), http://james.grimmelmann.net/files/articles/social-media-experiments.pdf.

[46] CCPA § 2(g) ("In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.").

[47] Article 29 Working Party, GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING UNDER REGULATION 2016/679 at 22 (Feb. 2018).

[48] *See, e.g.,* "FEDMA Code on E-Commerce & Interactive Marketing," FED. OF EURO. DIRECT MARKETING (2000), http://www.oecd.org/sti/ieconomy/2091875.pdf ("6.2 Marketers targeting children, or for whom children are likely to constitute a section of their audience, should not exploit children's credulity, loyalty, vulnerability or lack of experience.; 6.8.5 Marketers should not make a child's access to a website contingent on the collection of detailed personal information. In, particular,

The RFC's failure to address manipulation is a significant gap that again fails to create a substantive backstop on what companies may do to users. Secretly exploiting individuals' natural vulnerabilities not only distorts the market but threatens individual autonomy and to destroy any trust individuals may have in digital platforms and products.

B. Missing Principles

While based on the FIPPs, the RFC's Privacy Outcomes fully or partially omit several foundational data privacy principles.[49] In particular, the RFC omits collection limitation, data quality, purpose specification, individual participation, and privacy by design.[50]

A risk-based approach must complement, not replace, existing legal and regulatory frameworks. Risk-based flexibility is a method for achieving enhanced privacy protections, not a substitute for established principles. Even if organizations are permitted to tailor their accountability tools to the level of risk, these fundamental principles (transparency, control, reasonable minimization, security, access and correction) should not shift with risk-levels. While risk management is a mechanism for "operationalizing" "desired outcomes," it is not an end in itself.

i. Collection Limitation

The RFC conspicuously omits the principle of collection limitation. As the OECD explains:

> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[51]

Companies following this principle should not collect personal data indiscriminately. When they do gather personal data, they should do so lawfully, fairly, with an individual's knowledge, and subject to an individual's consent. This principle both obliges companies to limit data collection and grants notification and sometimes consent rights to people whose information is collected. Some kinds of particularly sensitive information, such as children's data or the content of phone calls, historically cannot be gathered at all without consent.

---

special incentives such as prize offers and games should not be used to entice children to divulge detailed personal information").

[49] We largely compare the Outcomes in the RFC to the OECD's Basic Principles. *See, e.g.,* Organisation for Economic Co-operation and Development, *The OECD Privacy Framework* (2013), at 14-15, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[50] While "privacy by design" is not part of the OECD FIPPs, we include it as an increasingly central principle of data practices. *See* GDPR, art. 25, https://gdpr-info.eu/art-25-gdpr/. *See generally* Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018).

[51] *OECD Privacy Framework* at 14.

The RFC, by contrast, does not state that companies should in general limit data collection. It proposes "Reasonable Minimization"—that is, that "data collection . . . should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm." This implies that if a company decides that there is no risk of privacy harm, it need not minimize data collection. That is in tension with the collection limitation principle, which applies no matter the context, and suggests that some kinds of information should not be gathered at all.

The RFC also fails to acknowledge the role of consent—an important feature of many existing privacy regimes, though not one that is sufficient by itself to protect privacy. The RFC does emphasize that users should have "reasonable control over the collection… of… personal information," but states that individual control "should depend on context."[52] This is not the principle of collection limitation; it is a context-specific suggestion that sometimes companies might want to provide individuals with control. The RFC does not clarify who is to determine that context; if it is companies that determine it, individuals will often get no right to consent to collection.

The principle of collection limitation is embodied in many US privacy laws, including the Electronic Communications Privacy Act;[53] state eavesdropping laws;[54] the Children's Online Privacy Protection Act and Rule;[55] video voyeurism laws, including the federal version;[56] and the Illinois Biometric Privacy Act.[57] These laws prohibit the collection of personal

---

[52] RFC, 83 Fed. Reg. at 48,601.

[53] Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(c) ("ECPA") ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.").

[54] *See, e.g.,* CAL. PENAL CODE § 632(a) (West 2010) (defining "[e]avesdropping" as when a person "intentionally and without . . . consent . . . eavesdrops upon or records . . . confidential communication"), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=632; COLO. REV. STAT. § 18-9-304(1)(a)-(c) (2016) (defining "[e]avesdropping" as when a person not present for a conversation "[k]nowingly overhears or records such conversation or discussion without . . . consent"), https://codes.findlaw.com/co/title-18-criminal-code/co-rev-st-sect-18-9-305.html.

[55] Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4 (requiring verifiable parental consent).

[56] 18 U.S.C. § 1801 ("(a) Whoever, in the special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both").

[57] Illinois Biometric Information Privacy Act, 740 ILCS 14/15 ("Sec. 15. Retention; collection; disclosure; destruction . . . (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it

information without consent. Other U.S. frameworks focus on providing meaningful transparency and choice in collection practices, particularly with newer technologies that violate individuals' situational expectations of privacy.[58] Supreme Court Fourth Amendment jurisprudence can also be understood as collection limitation applied to the government. This constraint has been applied in recent years to limit information collection through: the use of thermal imaging technology,[59] GPS sensors,[60] and cellphone location tracking capabilities.[61]

The lack of a generally applicable collection limitation principle in the RFC plays into the hands of companies that would rather not notify or obtain consent from individuals when collecting information. This shortcoming was at the core of the conflict over the NTIA's multi-stakeholder process on facial recognition, where civil society groups walked out of the process after companies refused to seriously consider collection limitations in the form of an opt-in, consent-based approach.[62] Without a robust principle of collection limitation, the NTIA risks ignoring, or worse, preempting both historic and newly developed protections against indiscriminate data collection, especially in physical (as opposed to digital) spaces.[63]

ii. Data Quality

The data quality principle imposes substantive obligations on companies to monitor the quality—including the relevance—of the data they hold. As the OECD explains

---

first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;").

[58] *See, e.g.*, Federal Trade Commission, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 10 (2012), 14-15 https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (An FTC facial recognition study, which emphasizes the principles of "privacy by design, simplified choice, and improved transparency" and noting that "providing a clear notice is particularly important because a digital sign or kiosk that contains a camera using facial recognition technologies will often look no different to a consumer than a digital sign that does not have a camera within the display . . . . Choice is important in these situations as well"; *see also* NAT'L TELECOMM. AND INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY (2016) https://www.ftc.gov/system/files/documents/public_comments/2016/10/00008-129242.pdf (NTIA best practices for drone use. Section 2(b) states that "In the absence of a compelling need to do otherwise, or consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of covered data about individuals.").

[59] Kyllo v. United States, 533 U.S. 27, 28 (2001).

[60] United States v. Jones, 565 U.S. 400, 404 (2012).

[61] Carpenter, 138 S. Ct. at 2217.

[62] Jennifer Lynch, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process*, EFF (June 16, 2015), https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi.

[63] Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. LAW REV. 57, 65 (2013), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1007&context=clrcircuit.

> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[64]

The RFC proposes putting the burden of maintaining data accuracy on individuals rather than companies.[65] While we applaud the notion of individual participation, including an individual correction right, putting the burden of maintaining data quality onto companies is increasingly important in the age of digital profiling, especially given the fairness concerns articulated above.[66]

The principle of data quality is embodied in US laws, including, for example, the Fair Credit Reporting Act, which imposes such requirements on consumer reporting agencies. Those agencies must follow procedures to assure data accuracy, and when accuracy is disputed, must reinvestigate and promptly delete inaccurate, incomplete, or unverifiable data from a consumer's file.[67]

Data quality also includes timeliness, meaning that data must be up-to-date and should not be retained for overly long periods of time. Under the FCRA, companies are not permitted to include in consumer reports certain categories of information dating back a certain number of years.[68]

Data quality requires that data be relevant. The RFC does not mention the importance of data relevance—that is, of not retaining more data than is necessary *for a particular purpose*. This missing requirement of data relevance connects to the next missing principle: of purpose specification.

iii. Purpose Specification

The principle of purpose specification is glaringly absent from the RFC. The principle of purpose specification helps make concrete other data privacy principles such as minimization, collection limitation, and use limitation. Data collection, use, and retention cannot be "minimized" if a company does not know or articulate the purpose for which collection, use, and retention of data occurs. Purpose specification is also a central component of effective

---

[64] *OECD Privacy Framework* at 14.

[65] RFC, 83 Fed. Reg. at 48,601.

[66] *See* discussion *supra* Part I.A.iii.

[67] FCRA, 15 U.S.C. § 1681e(b) ("Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual…").

[68] FCRA, 15 U.S.C. § 1691c(a) (preventing consumer reporting agencies from using bankruptcy proceedings more than ten years old; suits and judgments more than seven years old, paid tax liens more than seven years old, except under certain circumstances).

transparency, as disclosure policies often require that individuals be told the reasons for which their data are gathered and used.[69]

According to the OECD, purpose specification requires that:

> The purposes for which personal data are collected should be specified not later than at the time of data collection . . . .[70]

Purpose specification is central, for example, to the GDPR, which calls for data to be "collected for specified, explicit and legitimate purposes."[71] Determining the purpose of collection and processing can be as central to data protection law as individual notice and consent.[72]

Use limitation, another core principle of data privacy law—and one referenced in passing in the RFC's paragraph on "Reasonable Minimization"[73]—often depends on purpose specification.[74] As the OECD states, "the subsequent use [of gathered data must be] limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." The GDPR similarly requires that data not be "further processed in a manner that is incompatible with those [stated] purposes."[75] The purpose specifications a company makes at collection then determine what uses a company may make of that information.

These two principles, purpose specification and use limitation, to some extent operationalize the concept of contextual integrity discussed above by requiring that data gathered for a particular purpose in a particular context not be used for other unrelated purposes—at least not without providing new notice of and obtaining new consent for the new use. This principle of purpose specification is particularly important for sensitive data that people disclose in the context of trusted relationships.

---

[69] *See* discussion *infra*, Part II.A.

[70] Organization for Economic Cooperation and Development, *OECD Privacy Framework* (2013) at 14, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[71] GDPR, art. 5(1)(b).

[72] *See, e.g.,* Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws,* INSTITUT FÜR INTERNET UND GESELLSCHAFT (April, 26 2018), https://www.hiig.de/en/the-principle-of-purpose-limitation-in-data-protection-laws/

[73] RFC, 83 Fed Reg. at 48,601.

[74] Organization for Economic Cooperation and Development, *OECD Privacy Framework* (2013) at 14. *See* RFC, 83 Fed. Reg. at 48,601 (discussing use limitations).

[75] GDPR, art. 5(1)(b).

These principles are important because secondary uses—using data collected for one purpose for another—are at the heart of many privacy violations.[76] This is exacerbated by the use of persistent identifiers, which make it easy to merge records from multiple databases.[77]

Purpose specification and related use limitations are enshrined in U.S. law. The 1973 HEW report that produced the original version of the FIPPs and led to the enactment of the Privacy Act notes that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[78] As a result, use limitation is a central component of the Privacy Act.[79] The recently enacted California Consumer Privacy Act (CCPA) also creates a purpose specification requirement by requiring businesses to notify consumers both of the categories of information they collect and the purposes for which they collect them.[80] Once a business has disclosed the purpose of collection, it "shall not … use personal info collected for additional purposes without providing the consumer with notice."[81]

Purpose specifications can be created by companies themselves. For particularly sensitive information, however, purpose specifications and related use limitations are often mandated by law. For example, HIPAA's requirement that covered entities obtain authorization before the use of health information for certain purposes can be understood as a statutorily mandated purpose specification and use limitation.[82] The FCRA also contains a list of permissible purposes for consumer reports and requires that those receiving reports certify that they will use them only for permissible purposes.[83]

---

[76] *See* Stephen Kent & Lynette I. Millett, Editors, *Who Goes There: Authentication Through the Lens of Privacy* (2003), at 97.

[77] *See* Steve Bellovin, *Replacing social security numbers is harder than you think*, VICE MOTHERBOARD (Oct. 5, 2017), https://motherboard.vice.com/en_us/article/pakwnb/replacing-social-security-numbers-is-harder-than-you-think; Steve Lohr, *A 10-Digit Key Code to Your Private Life: Your Cellphone Number*, NEW YORK TIMES (Nov. 12, 2016), https://www.nytimes.com/2016/11/13/business/cellphone-number-social-security-number-10-digit-key-code-to-private-life.html.

[78] U.S. Dep't of Health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems* 29-30, 41-42 (1973) ("HEW Report").

[79] *See, e.g.*, 5 U.S.C. § 552a(a)(7)"the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected"; (3)(4)(D) (requiring the publication of each routine use in a systems of records notice)

[80] CCPA § 1798.100(b).

[81] CCPA § 1798.100(b).

[82] HIPAA regulations, 45 C.F.R. § 164.508 ("Uses and disclosures for which an authorization is required"); HIPAA regulations, 45 C.F.R. § 164.512 ("Uses and disclosure for which an authorization or opportunity to agree or object is not required").

[83] FCRA, 15 U.S.C. § 1681(b).

iv. Individual Participation

The RFC superficially acknowledges the need for individual access and correction rights, also known as rectification rights, in addition to individual rights to complete, amend, and sometimes delete data, but "qualifie[s]" these rights by requiring their provision only when "reasonable, given the context" and given risks of privacy harms.[84] Setting a fuzzy standard and delegating to companies the decision over when individual rights should be provided is as bad as protecting no individual rights at all.

In addition, the principle of individual participation requires more than the individual rights of access, rectification, erasure, and amendment. As articulated by the OECD, it contains procedural requirements that access to data must be given "within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner, and; in a form that is readily intelligible."[85] Individuals must be given reasons that a request is denied and be able to challenge denials. NTIA should establish both concrete substantive and procedural requirements around these individual participation rights.

v. Privacy by Design

Privacy by design—the notion that privacy should be built into new data collection technologies from the ground up as part of the corporate ethos, practice, and routine of technology product design—is integral to any contemporary approach to privacy. We note that while the RFC mentions privacy by design and several design principles in passing, it is not listed among the stated Privacy Outcomes and does not appear to be central to the proposed approach.

There are multiple benefits to privacy by design, especially if NTIA seeks to replace a notice-and-choice regime with an outcome-based approach geared at protecting individuals in practice. Privacy by design addresses technologies before they cause harm, alleviates burdens from consumers who do not have the capacity to protect themselves from data risks, and reorients corporate habits toward meaningful compliance with the law of privacy, while retaining sufficient flexibility to spur innovation.

There are a variety of definitions of privacy by design: [86]

- The FTC has stated that privacy by design refers to companies "promot[ing] consumer privacy throughout their organizations and at every stage of the development of their

---

[84] RFC, 83 Fed Reg. 48,602.

[85] *OECD Privacy Framework*, (2013) at 15, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[86] The original seven Privacy by Design principles, developed by Ann Cavoukian, the former privacy commission for Ontario, Canada and a founder of the "PbD" program, echo the principles of user control and transparency that run throughout the FIPPs. Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (2011), https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. Cavoukian's provides clarification and guidance on applying the following 7 principles of privacy by

products and services."[87] The FTC has required companies to adopt privacy programs that include design considerations. For example, in 2011, the FTC required Google to "design and implement . . . reasonable privacy controls and procedures" in response to a privacy risk assessment.[88]

- Some connect privacy by design to privacy-enhancing technologies, or engineering tools that translate specific data protection principles into code.[89] This has led to calls for a design agenda for privacy regulation that would, for example, respond to the way technology companies design interfaces, agreements, and click boxes to manipulate, nudge, and encourage individuals to acquiesce to extensive data collection and use.[90]
- Others suggest that privacy by design includes organizational measures that integrate privacy professionals into a technology company's various business units, or integrate lawyers and privacy professionals into design teams.[91] Companies should integrate lawyers and privacy professionals into design teams and acculturate designers themselves into the ethos of privacy and ethics in design.[92]

In summary, privacy by design can refer to: technical measures, organizational measures, and regulatory approaches that try to bake privacy principles into both technologies themselves and corporate infrastructure, as an innate goal rather than a later add-on.

---

design: Proactive not Reactive; Privacy as a Default Setting; Privacy Embedded into Design; Full Functionality; End-to-End Security; Visibility and Transparency; and Respect for User Privacy.

[87] Federal Trade Commission, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE at vii. (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[88] FTC Consent Order, *In the Matter of* GOOGLE INC., File No. 102 3136 (2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf; *see also* F.T.C. v. Frostwire LLC, No. 1:11-CV-23643, 2011 WL 9282853 (S.D. Fla. 2011) (describing default setting of Android application that allowed sharing of all existing files on the device in terms of "unfair design").

[89] Ira S. Rubenstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1341 (2013), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj. By way of example, Rubinstein and Good explain that privacy by design should require companies not merely to promise to delete user data after a limited amount of time, but rather to design a database that automatically identifies personal information and deletes it at a pre-programmed date.

[90] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018).

[91] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), https://www.stanfordlawreview.org/print/article/privacy-on-the-books-and-on-the-ground/.

[92] *See* Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age (2018).

This approach to privacy has several advantages. First, it reflects the importance of fairly allocating responsibility for protecting personal privacy. Current privacy law, based on the myth of control and extracted consent, forces unprepared users to bear the burden of protecting their information in the face of manipulative design.

Second, privacy by design can be clear, yet flexible. It provides a governing structure and some level of certainty as to what the law requires, without mandating specific designs, thus allowing for innovation. Designers should choose a reasonably alternative privacy-protective design when one exists.

Third, despite its flexibility, privacy by design nevertheless places limits on predatory, opportunistic corporate behavior. Absent a requirement to consider privacy during design and to market only those products that achieve similar goals with privacy-protecting tools, dangerous technologies make their ways to unsuspecting and unequipped consumers who are left with limited recourse only after-the-fact.

Privacy by design does have its critics. Because privacy by design is "an amorphous concept", in some instantiations it can fail to provide clear guidance to engineers.[93] Some regulatory discussion, such as an FTC staff report,[94] "is best read as a first cut at agency guidance"[95] rather than anything precise.

C. Missing Trends

Any policies set by NTIA should reflect not just longstanding principles, but the recent development of several important and emerging points of consensus on data privacy. NTIA should recognize expanding definitions of Personally Identifiable Information (PII), the increasing recognition of privacy expectations in public, concerns over inferences arising from data analytics, and the governance of third parties that access and process consumer data.

i. The Expanding Definition of Personally Identifiable Information (PII)

NTIA should adopt a sufficiently broad definition of personally identifiable information to reflect the reality of data analytics and the failures of data anonymization. The concept of PII has formed the underpinning of many contemporary consumer privacy regimes, both within the United States and abroad.[96] Under this approach, U.S. federal privacy statutes largely apply to PII, and companies that anonymize data are largely exempt from regulation.

---

[93] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 at 1421 (2011).
[94] Bureau of Consumer Protection, Federal Trade Commission, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[95] *See* Rubinstein, *supra* n.93.
[96] Seth Schoen, *What Information is "Personally Identifiable"?*, EFF (Sept. 11, 2009), https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable.

However, it has become increasingly clear that data anonymization is not the silver bullet it was once thought to be.[97] Purportedly anonymous information can often be easily used to re-identify a specific person. For example, 87 percent of the American population can be identified based on the combination of ZIP code, birth date (including year), and sex.[98] Other types of information—such as search history or content ratings—can similarly be easily used to re-identify individuals in what many privacy regimes would currently consider anonymized databases.[99] In 2011, researchers showed that they could determine a person's Social Security Number from available pictures on a dating website using facial recognition technology to identify that person and cross-reference with information on his or her Facebook profile.[100]

Regulatory regimes have recently responded to the failures of anonymization by broadening the definition of what constitutes PII to include information that could indirectly or through inference identify an individual. For example, the CCPA provides what is likely the most comprehensive definition of personally identifiable information put forward by any regulatory body to date. The CCPA includes in its definition of "personal information" not just information that identifies a consumer, but information that "is capable of being associated with, or could reasonably be linked . . . with a particular consumer or household."[101] This prevents companies from pretending to have anonymized personal data while in practice being fully aware of what information belongs to whom.

The CCPA contains a long and non-exhaustive list of what constitutes personal information, aimed at preventing companies from evading regulation by creating proxies for identity. That list includes:

> Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers [including] [b]iometric information…browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement[,] . . .

---

[97] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L. REV. 1701, 1732 (2010) ("The idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned."); *see also, e.g.*, *In Re Hulu Privacy Litigation*, 2014 WL 1724344 (N.D. Cal. 2014) (finding that an anonymized ID could be "the equivalent to the identification of a specific person," but failing to protect user privacy under the VPPA).

[98] Ohm, *Broken Promises of Privacy*, 57 UCLA L. REV. at 1705.

[99] *Id.*

[100] Kashmir Hill, *How Facial Recognition Technology Can Be Used To Get Your Social Security Number,* FORBES (Aug. 1, 2011), https://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/.

[101] CCPA § 1798.140(o)(1).

> [g]eolocation data[,] . . . [a]udio, electronic, visual, thermal, olfactory, or similar information . . . .[102]

Moreover, the CCPA includes in its definition of PII "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer."[103] This extends privacy protection not just to information gathered about a consumer, but to sensitive information inferred about a consumer by a company.

The GDPR also robustly defines "personal data" as "any information relating to an identified or identifiable natural person"[104] It clarifies that "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[105]

Similar to the CCPA, the GDPR seeks to alleviate concerns about the success of re-identification of anonymized data by including the language "directly or indirectly" to broaden how information can be used to identify an individual. Both the text of the GDPR and Recital 26 make clear that merely removing identifying information from a data set is not enough to address individual privacy concerns.[106]

In addition to these protections, the GDPR—like the CCPA—includes a specific list of identifying information that the regulation protects. This information includes identifiers and location data, as well as factors specific to "the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person."[107]

The GDPR provides additional protections for "special categories" of personal data. The GDPR expressly prohibits "[p]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[108]

The recent Supreme Court decision in *Carpenter* suggests that U.S. courts, too, are beginning to take on a more expansive understanding of what constitutes personal data.[109] In *Carpenter*, the Court addressed whether a search occurred when police accessed historical cell phone records

---

[102] CCPA § 1798.140(o)(1)(A-K).
[103] CCPA § 1798.140(o)(1)(K).
[104] GDPR, ch. 1, art. 4(1).
[105] GDPR, ch. 1, art. 4(1).
[106] GDPR, recital 26(2).
[107] GDPR, ch. 2, art. 4(1).
[108] GDPR, ch. 2, art. 9(1).
[109] Carpenter, 138 S. Ct. at 2246.

that provided a comprehensive record of the user's location.[110] The Court held that individuals have a reasonable expectation of privacy in the record of their physical movements as captured by historic cell site location information, and thus that accessing such records does constitute a search.[111]

The Court reasoned in *Carpenter* that location data, which in earlier cases had not been considered private information, now constitutes sensitive information because sensitive inferences can be made from it. "As with GPS location, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, profession, religious, and sexual associations.'"[112] This concern mirrors the GDPR's protection of "special categories" of personal data. Even Justice Kennedy's dissent in *Carpenter* connects financial and telephone records through inferences to information about somebody's "personal affairs, opinions, habits, and associations."[113]

ii. Privacy in Public

While it has long been a platitude in U.S. law that people do not have an expectation of privacy in public—and an arguably legally incorrect platitude under, for example, *Katz v. United States*[114]—a series of recent legal developments fundamentally challenge this idea. As discussed above, the Supreme Court in *Carpenter* found an expectation of privacy in historic location information, even though it was revealed in public places.[115] And as noted above, location information is among the categories of personal information listed in both the CCPA and the GDPR.[116] Biometric information, including facial recognition data, is also protected as personal information in both the GDPR and the CCPA.[117]

Recognizing that individuals can have an expectation of privacy in public conflicts with an array of current data practices. Companies gather license plate information, biometric information, and video footage from public spaces. They largely do so under a now-outdated assumption that information revealed in public cannot also be private.[118]

---

[110] *Id.* at 2211.
[111] *Id.* at 2222.
[112] *Id* at 2217.
[113] *Id.* at 2232.
[114] 389 U.S. 347, 351 (1967) (famously suggesting that the Fourth Amendment protects "people, not places").
[115] *See* discussion *supra*, Part I.C.i.
[116] GDPR, ch. 1, art. 4(1).
[117] CCPA § 1798.140(o)(1).
[118] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public,* Law and Philosophy, vol. 17, no. 5/6 (1998); Joel R. Reidenberg, *Privacy in Public,* 69 UNIV. OF MIAMI L. REV 141 (2014); Margot E. Kaminski, Regulating Real-World Surveillance, 90 WASH. L. REV. 1113 (2015).

NTIA's multistakeholder best practices for drone (UAS) use reflect this assumption that data loses its sensitive nature depending on where it is revealed.[119] Drone operators under these best practices agree not to collect personal data "*where* the operator knows the data subject has a reasonable expectation of privacy."[120]

After *Carpenter*, and under the GDPR and California CCPA, the question is not "where" but "what." Sensitive information such as location information may be gathered even in locations not historically deemed to be private. To the extent NTIA is interested in harmonization with Constitutional, state, and international law, it should acknowledge this shift in approach to information revealed in public spaces, by recognizing that people clearly can now have an expectation of privacy in public.[121]

iii. Big Data Analytics and Inferences

Closely related to the growing understanding that information revealed in public can be private is the growing consensus that non-sensitive information can become sensitive information through data analytics. In other words: the inferences revealed by data analysis can be sensitive, even when underlying data are not.

The Court's reasoning in *Carpenter* followed exactly this logic: location information, which had not been considered inherently sensitive information, became sensitive in nature because when gathered in quantity it could "reflect[] a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[122] Thus, inferred information, including inferred location information, can receive constitutional privacy protection. The GDPR also covers inferences,[123] as does the CCPA.[124]

NTIA should likewise recognize that inferred data often has the same characteristics as personal data, and that large quantities of non-sensitive information, when analyzed, can give rise to sensitive personal information.

---

[119] NAT'L TELECOMM. AND INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY at 8 (2016), https://www.ftc.gov/system/files/documents/public_comments/2016/10/00008-129242.pdf.

[120] *Id.* at 5-6 (emphasis added).

[121] *See* Ira Rubinstein, *Privacy Localism*, NYU School of Law, Public Law Research Paper No. 18-18 (2018), https://ssrn.com/abstract=3124697 (discussing local surveillance ordinances in cities such as Seattle and Oakland that seek to protect privacy in public settings).

[122] Carpenter, 138 S. Ct. at 2217.

[123] Article 29 Working Party, GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING UNDER REGULATION 2016/679 at 7 (Feb. 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (Guideline says inferences are included.)

[124] CCPA § 1798.140(o)(1)(K) "(K) Inferences drawn from any of the information… to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

iv. Extending Regulation to Third Parties Including Data Brokers

As the FTC noted in its 2014 report on data brokers, U.S. privacy enforcement struggles to reach third parties unless those entities or their practices fall under a specific sectoral regime such as the Fair Credit Reporting Act.[125] This has led to an unregulated shadow industry of data brokers that provide little to no transparency in their practices, let alone adequate legal recourse for individuals whose data they collect.

Recent trends suggest that this lack of regulation is ending. The GDPR explicitly regulates companies that hold individuals' personal data, regardless of whether they have a direct business relationship with those individuals. For example, the GDPR imposes affirmative notice requirements on companies "where personal data have not been obtained from the data subject."[126] Protections, including subject access and rectification rights, follow the data, rather than focusing only on regulating direct relationships between consumers and companies.[127]

Bringing transparency to data broker practices is in an explicit goal of the California Consumer Privacy Act.[128] The CCPA's transparency provisions apply not just to businesses that have a direct relationship with consumers, but to all businesses that collect personal data, whether or not they obtain that personal data from a consumer.[129] Like the GDPR, the CCPA's transparency provisions follow the data, not the relationship. The CCPA also targets data brokers by giving consumers the right to opt out of having information sold by one business to another.

The Supreme Court's rejection of third party doctrine in *Carpenter* indicates a similar decision to protect location information as it flows from cell phone providers to the government. This again focuses on protecting the data as sensitive data, regardless of whether it is obtained directly from an individual or through another entity.

---

[125] Federal Trade Commission, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[126] GDPR, art. 14.

[127] William McGeveran, *Friending the Privacy Regulators,* 58 ARIZ. L. REV. 959, 964 (2016).

[128] CCPA § 2(g) and § 2(i)(1-2) ("In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica…Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights…
(1) The right of Californians to know what personal information is being collected about them….
(2) The right of Californians to know whether their personal information is sold or disclosed and to whom . . .").

[129] CCPA § 1798.140(e) ("'Collects,' 'collected,' or 'collection' means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior").

NTIA should recognize the need for transparency in data broker practices and regulate data broker practices such as the sale of consumer information, consistent with the trend of applying data privacy regulation to third parties.

II. Implementing Data Privacy Principles in Effective and Protective Ways

The RFC moves away from notice-and-choice and towards a focus on privacy outcomes.[130] Individuals are often practically disempowered when it comes to data practices, and leaning too heavily on individual capabilities can lead to no privacy in practice.

However, building data policy around high-level principles risks being vague, aspirational, and equally ineffective. Below, we provide concrete examples to guide NTIA practices in implementing the principles of transparency, access and correction, accountability, control/consent, and risk management. As examples, we draw on existing federal regulation, state laws, and the EU's GDPR.

A. Making Transparency Effective

The RFC calls for transparency, in the sense that "[u]sers should be able to easily understand how an organization collects, stores, uses, and shares their personal information."[131] While transparency is not by itself a sufficient approach to privacy, effective transparency in conjunction with other measures remains central to traditional data privacy law. It empowers users through individual participation, and provides needed oversight and accountability over company practices through openness and accountability. Transparency is not a new construct in data privacy law.

Here, we here provide examples from a number of regulatory regimes—HIPAA, COPPA, FCRA, and the GDPR—that illustrate how to concretize transparency requirements and make transparency more effective. These existing data privacy regimes have created a number of requirements for effective transparency, whether through law, regulation, or guidance.

First, information provided to consumers should be "**clear and conspicuous**" and in writing:

- The Fair Credit Reporting Act ("FCRA"), for example, requires that a person "may not procure a consumer report, or cause a consumer report to be procured for employment purposes unless -- (i) a clear or conspicuous disclosure has been made in writing to the consumer . . . ."[132]
- The GDPR Guidelines on Transparency explain that companies "should present information/communication efficiently and succinctly in order to avoid information

---

[130] RFC, 83 Fed. Reg. at 48,601.

[131] *Id.*

[132] FCRA, 15 U.S.C. § 1681(b)(2)(A)(i).

fatigue."[133] To achieve this, privacy-related information should be clearly differentiated from other contractual provisions, such as terms of use.

Next, information provided to consumers should be **understandable**:

- The Children's Online Privacy Protection Act (COPPA) requires that notice to children "must be clearly and understandably written, complete, and contain no unrelated, confusing, or contradictory materials."[134]
- Under the GDPR, this requirement extends beyond children. Article 12 requires that information given to individuals must, among other requirements, be ". . . concise, transparent, intelligible and easily accessible."[135] Conveyed information should be "user-centric rather than legalistic," and the "quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information."[136]

Third, information provided to consumers should be available in a **clear and prominent location** as a matter of design:

- COPPA requires that web or online service providers "post a prominent and clearly labeled link to an online notice of its information practices on the home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service where personal information is collected from children."[137]
- HIPAA requires that notice of privacy practices for protected heath information be posted "in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice."[138]
- The GDPR Guidelines emphasize that a company "must take active steps to furnish the data in question to the data subject, or to actively direct the data subject to the location of it . . . ."[139] If appropriate, the GDPR allows information related to data processing to be conveyed via "visuali[z]ation tools," including icons, certification, and data protection seals and marks.[140]
- The California CPA contains specific details of how a privacy notice and privacy rights must be presented. They must be "reasonably accessible to consumers," which includes a

---

133 Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679* at 7 (April 11, 2018) ("A29WP Transparency Guidelines"), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

134 COPPA regulations, 16 C.F.R. § 312.4(a).

135 GDPR, art. 12(1).

136 *Id.*

137 COPPA regulations, 16 C.F.R. § 312.4(4)(d).

138 HIPAA regulations, 45 C.F.R. § 164.520.

139 A29WP Transparency Guidelines at 18.

140 *Id.* at 25.

number of detailed requirements, including establishing a link that states "Do Not Sell My Personal Information."[141]

Fourth, information provided to consumers should be **substantive:**

- As a requirement for obtaining written authorization, HIPAA requires the disclosure of very specific elements, including a description of the information, the recipients of information, the purpose of use, and more.[142] A HIPAA authorization also must include notice of the individual's right to revoke the authorization in writing, whether or not the treatment, payment enrollment, or eligibility may be conditioned on authorization under HIPAA, and the potential for information to be disclosed pursuant to the authorization.[143]
- The CCPA requires that both disclosures and responses to access requests include a specific list of required information. Disclosures must include, among other things: a description of consumer's rights, a "list of categories of personal info by enumerated category," and a list of the categories of information a business has sold.[144] Additionally, consumers must be granted access to specific pieces of personal information, categories of personal information collected about them, categories of the sources from which information has been collected, and more.[145]
- The GDPR also contains deep, specific requirements on substance. Article 13 requires that, when personal data is collected, a company must provide a long list of specific information, including but not limited to, the purposes of processing, the recipients of

---

[141] CCPA § 1798.130, 1798.135.

[142] HIPAA regulations, 45 C.F.R. § 164.508(c)(1)(i-iv) ("(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure. (iii) The name or other specific identification of the person, or class of person(s), to whom the covered entity may make the requested use or disclosure. (iv) […] The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose. (v) […] The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research depository. (vi) […] If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be provided").

[143] HIPAA regulations, 45 C.F.R. § 164.508(c)(2)(i-iii).

[144] CCPA § 1798.130(5).

[145] CCPA § 1798.110(a)(1) (categories of personal info it has collected about THAT consumer; (2) categories of sources form which the info is collected; (3) commercial or business purpose for collecting or selling info; (4) categories of third parties with whom info is shared; (5) specific pieces of personal info it has collected about that consumer).

data, and both the fact of and explanation of profiling and automated decision-making.[146] It also requires disclosing the period of time for which data will be stored, and the existence of a number of individual rights with respect to the data, among other things.[147] Article 14 requires that companies provide nearly identical information even when personal data has not been obtained from the data subject.[148]

- The GDPR additionally contains a requirement that requires companies disclose "meaningful information about the logic involved" in automated decision-making.[149]

Finally, information provided to consumers should be **timely:**

- FCRA requires disclosure to a consumer before a consumer report can be procured.[150]
- HIPAA similarly requires disclosure prior to authorization.[151]
- The CCPA requires notice at or before the time of collection (or up to within 90 days under certain circumstances).[152]
- Under the GDPR Article 13, disclosures must be made at the time information is collected.[153] Disclosures under Article 14 must occur "(a) within a reasonable period after obtaining the personal data, but at the latest within one month . . . ; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, a the latest when the personal data are first disclosed."[154] The GDPR's transparency requirements are not static, but ongoing.

---

[146] GDPR art. 13(1) ("(a) the identity and contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission […] reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.").

[147] GDPR art. 13(2).

[148] GDPR art. 14(1-3).

[149] GDPR art. 15(1)(h).

[150] FCRA regulations, 16 C.F.R. § 640.4(a)(1).

[151] HIPAA regulations, 45 C.F.R. § 164.508(a)(1).

[152] CCPA § 1798.100(b).

[153] GDPR, art. 13(1) ("at the time when personal data are obtained").

[154] GDPR, art. 14(1-3).

B. Making Access and Correction Rights Effective

The RFC states that "[u]sers should have qualified access [to] personal data that they have provided, and to rectify, complete, amend, or delete this data."[155] This right of individual participation again is not new. Here, we provide examples of how to concretize individual participation rights from: the OECD principles, the GDPR, the FCRA, COPPA, California's Privacy Rights for California Minors in the Digital World, the California CPA, HIPAA, and with respect to government records, the Privacy Act. These regimes have created a number of requirements for effective access and correction rights.

First, the right to access should be **easy:**

- The OECD explains that the right to access should be a simple exercise that should not involve legal process.[156] A company should provide information to an individual within reasonable time considering the bandwidth the controller has in processing individual requests.[157]
- The FCRA, COPPA, HIPAA, and the Privacy Act each have a version of access that reflects the need for ease of accessibility.[158]

Second, the information made accessible should be disclosed in a **usable format**:

- Under the Privacy Act, which applies to federal agencies, an agency that maintains a system of records must permit any individual requesting access to have a copy made of a record or portion of a record in a form comprehensible to him or her.[159]
- The CCPA requires that such information be delivered in a readily useable format free of charge to the consumer.[160]
- Under HIPAA, covered entities must provide the individual with access to their information in the form and format requested by the individual, if it is readily producible in that form; or, if not, in a readable hard copy form.[161]
- The GDPR requires data portability: i.e., that an individual has "the right to receive the personal data concerning him or her, which he or she has provided to a [company], in a

---

[155] RFC, 83 Fed. Reg. at 48,602.

[156] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paragraph 59, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[157] *Id.*

[158] *Id.*

[159] Privacy Act of 1974, 5 U.S.C §552a(d)(1).

[160] CCPA § 1798.100(d).

[161] HIPAA regulations, 45 C.F.R. § 164.524(c)(2)(i).

structured, commonly used and machine-readable format and have the right to transmit those data to another [company] without hindrance."[162]

Third, the right of access should be **substantively deep**:

- The FCRA allows a consumer to access and control some of the information held by consumer reporting agencies. Upon request, a consumer reporting agency is required to disclose all information in the consumer's file at the time of the request.[163] The agency must disclose the sources of credit report information and the identification of each person that procured a consumer report about the consumer filing the request.[164]
- Under COPPA, a web site operator must provide a description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities.[165]
- The CCPA provides that a consumer has the right to request access to the categories and specific pieces of personal information the business has collected about them.[166] Specifically, a business must disclose upon request:
    1. The categories of personal information it has collected about that consumer;
    2. The categories of sources from which the personal information is collected;
    3. The business or commercial purpose for collecting or selling personal information;
    4. The categories of third parties with whom the business shares personal information; and
    5. The specific pieces of personal information it has collected about that consumer.[167]
- These closely parallel the kinds of information required to be disclosed by Article 15 of the GDPR.[168]
- Under HIPAA, individuals have a right to access Personal Health Information ("PHI") comprising medical records and billing records; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or other records that are used by the covered entity to make decisions about individuals.[169]

---

[162] GDPR, art. 20.
[163] FCRA, 15 U.S.C. § 1681g(a).
[164] FCRA, 15 U.S.C. § 1681g(a)(3)(A).
[165] COPPA, 16 C.F.R. § 312.6(a)(1).
[166] CCPA § 1798.100(a).
[167] CCPA § 1798.110(a).
[168] GDPR, art. 15.
[169] HIPAA regulations, 45 C.F.R. § 164.501.

Finally, individuals should have a right of **correction, also known as rectification:**

- The FCRA gives consumers rights similar to the "right to rectification" outlined in Article 16 of the GDPR. Under the FCRA, if a consumer disputes the accuracy or completeness of the information contained in the consumer's file the consumer may notify the consumer reporting agency of the discrepancy.[170] After receiving this notification, the consumer reporting agency must conduct a reinvestigation to determine whether the disputed information is inaccurate, record the current status of the disputed information, or delete the disputed information altogether.[171]
- Under HIPAA, an individual may request for the covered entity to amend incorrect or incomplete information in their file.[172] The covered entity has 60 days to act on such a request[173] and may deny amendment if the information was not created by the covered entity; if the information is not part of the individual's designated record; is not the kind of information which may be accessed; or is already accurate and complete.[174]
- The Privacy Act provides individuals the right to amend records, albeit only with respect to federal government agencies.[175] After an individual requests to amend her record, the agency holding the individual's records must promptly either make any correction the individual believes is not accurate or complete or inform the individual of its refusal to amend.[176] If the request for amendment is refused, the agency must disclose the reason for the refusal and the procedures established by the agency for the individual to request a review by the head of the agency.[177]
- The FCRA gives consumers rights similar to the 'right to rectification' outlined in Article 16 of the GDPR. Under the FCRA, if a consumer disputes the accuracy or completeness of the information contained in the consumer's file the consumer may notify the consumer reporting agency of the discrepancy.[178] After receiving notice, the consumer reporting agency must conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate, record the current status of the disputed information, or delete the disputed information altogether within 30-days of notice of the dispute.[179]

---

[170] FCRA, 15 U.S.C. § 1681i(a)(1).
[171] FCRA, 15 U.S.C. § 1681i(a)(1)(A).
[172] HIPAA regulations, 45 C.F.R. § 164.526.
[173] HIPAA regulations, 45 C.F.R. § 164.526(b)(2)(i).
[174] HIPAA regulations, 45 C.F.R. § 164.526(a)(2)(i-iv).
[175] Privacy Act of 1974, 5 U.S.C § 552a.
[176] Privacy Act of 1974, 5 U.S.C § 552a(d)(2)(B).
[177] Privacy Act of 1974, 5 U.S.C. § 552a(d)(2)(B)(ii).
[178] FCRA, 15 U.S.C. § 1681i(a)(1).
[179] FCRA, 15 U.S.C. §1681i(a)(1)(A).

C. Addressing Control/Consent

The RFC calls for control of information in that "[u]sers should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations." This notion of "control" relates directly to the idea of receiving appropriate consent to use an individual's personal information.

Consent, while insufficient on its own to protect privacy, is nevertheless important in conjunction with other measures. Broadly speaking, consent involves four key features:

- Clear background conditions for permissible and impermissible uses of one's data;
- A defined scope of action for the applicable consent;
- Knowledge by the data subject of what the subject is consenting to and what subject's options are; and
- The freedom to choose from the range of options.[180]

Existing data privacy regimes have created several approaches to effective consent.

First, many existing regimes require that consent be **clearly and affirmatively obtained, often in writing:**

- COPPA requires parental consent and allows companies to choose the best method to obtain proper parental consent, but recommended methods of verifying that consent is obtained from a parent include: signing and sending a consent form; calling a toll-free number staffed by trained personnel; answering a series of "knowledge-based challenge questions" aimed at verifying the parent's identity; and verifying a picture of the parent's driver's license, among other possible methods.[181]
- Under the Family Educational Rights and Privacy Act (FERPA), student data similarly may not be transferred to third parties without the written consent of the parent of the student.[182]
- Article 4(11) of the GDPR defines consent as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes that he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[183] Consent must be given unambiguously in the form of a "statement or by a

---

[180] Meg Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 1, 9 (2018) (draft manuscript).
[181] *Id.*
[182] 20 U.S.C. § 1232g(b)(4)(B).
[183] GDPR, art. 4(11); *see also* A29WP: A29 WP, GUIDELINES ON CONSENT UNDER REGULATION, 17/EN. WP59, ("A29WP Consent Guidelines") (April 10, 2018), https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en. 4.

clear affirmative action."[184] This must be obtained through the subject's "deliberate action to consent to the particular processing."[185]

- According to the GDPR Guidelines on Consent, "pre-ticked opt-in boxes" are invalid forms of consent, as are a data subject's silence or inactivity.[186] Blanket acceptance of general terms and conditions is not "clear affirmative action to consent to the use of personal data."[187] The Guidelines note that companies "should design consent mechanisms in ways that are clear to [an individual]."[188] Consent mechanisms should be unambiguous, and should be easily distinguished from other actions.[189] "[C]ontinuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data to signify his or her agreement to a proposed processing operation."[190] For example, designing a button to decline consent that is unnecessarily tiny, or that is hidden within the regular operations of an online good or service, would not satisfy the consent requirement under the GDPR.[191] The GDPR contains even more stringent consent requirements for (a) children's data and (b) special category or otherwise high risk data.[192]

Second, under many regimes, consent must be **informed**, and the notion that consent should be "informed" is central to understanding consent more generally:

- For authorization of use of health information to be valid under HIPAA, it must contain a long list of specific elements, including a description of the information, the recipients of information, the purpose of use, and more.[193]

---

184 A29WP Consent Guidelines at 15; *see also*, GDPR, art. 4(11).

185 A29WP Consent Guidelines at 16; *see also*, GDPR, recital 32.

186 A29WP Consent Guidelines at 16.

187 A29WP Consent Guidelines at 16; *see also*, GDPR art. 7(2).

188 A29WP Consent Guidelines at 16.

189 *Id.*

190 *Id.*

191 *See* Josh Constine, TECHCRUNCH, "A flaw by flaw guide to Facebook's new GDPR privacy changes," (April, 2018) (Facebook's tiny button that allows a consumer to "See Your Options" in choosing to accept or reject their new terms of service), https://techcrunch.com/2018/04/17/facebook-gdpr-changes/.

192 A29WP Consent Guidelines at 18, 23-24; *see also* GDPR, arts. 8(1), 9, 22, 49.

193

> "(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure. (iii) The name or other specific identification of the person, or class of person(s), to whom the covered entity may make the requested use or disclosure. (iv) . . . The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the

- Under COPPA, companies must obtain verifiable parental consent before collecting any information about children under the age of thirteen.[194] This involves first giving "direct notice" to parents regarding information practices before collecting information from their kids.[195] The notice should be easy to read, should not include unrelated or confusing information, and must tell parents: "that you want to collect their online contact information for the purpose of getting their consent; that you want to collect personal information from their child; that their consent is required for the collection, use, and disclosure of the information; the specific personal information that you want to collect and how it might be disclosed to others; a link to your online privacy policy; how the parent can give their consent; and that if the parent doesn't consent within a reasonable time, you'll delete the parents contact information from your records."[196]
- As discussed in the section on Transparency above,[197] companies must offer in-depth and specific information to individuals under the GDPR.[198] The information may be provided in numerous ways as long as the method chosen "leads to a higher standard for clarity and accessibility of the information."[199]

Third, some existing regimes require that consumers be **offered a genuine choice**:

- The Guidelines on Consent under the GDPR establish that "consent can only be a lawful basis [for processing data] if a[n individual] is offered control and is offered a genuine choice with regard to accepting or declining the terms offered, or declining them without detriment."[200] Article 7(4) of the GDPR specifically notes that "bundling" consent to the acceptance of terms and conditions means the consent is presumptively not freely

---

> authorization and does not, or elects not to, provide a statement of the purpose. (v) . . . The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research depository. (vi) . . . If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be provided." 45 C.F.R. §164.508(c)(1)(i-iv).

194 Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, (June, 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

195 *Id.*

196 Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business.*

197 *See* discussion *supra* Part II.A.

198 GDPR, art. 13-14.

199 A29WP Consent Guidelines at 14; *see also* GDPR, art. 7(2) & recital 32.

200 A29WP Consent Guidelines at 3.

given.[201] "Consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or provision or the provision of a service."[202] The GDPR encourages data controllers to avoid "conditional services," which force customers' to give consent to the processing of their personal data in exchange for the service.[203]

- Similarly, under COPPA, companies must give parents the option of allowing collection of their children's information "without agreeing to disclose that information to third-parties.[204]

Fourth, some existing regimes require that individuals be permitted to **withdraw consent**:

- HIPAA authorization must include notice of the individual's right to revoke the authorization in writing.[205]
- Article 7(3) of the GDPR establishes that a company "must ensure that consent can be withdrawn by [an individual] as easy as giving consent and at any time."[206] Consent is not free if an individual cannot withdraw or refuse consent without negative consequences.[207]

Fifth, some existing regimes prohibit companies from **penalizing** consumers for withholding or withdrawing consent, for example by conditioning the provision of services on consent:

- The California CPA has a nondiscrimination provision aimed at prohibiting companies from discriminating against consumers that exercise a right to decline consent.[208]
- The GDPR emphasizes the need for an individual to be able to withdraw consent easily, without additional charge, and without lowering service levels.[209]

Sixth, where consent is not provided, some existing regimes **allow consumers the ability to opt out**. While the CCPA does not require consent, it does allow Californians to, at any time, "direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information." [210] This is referred to as the "right to opt out."[211]

---

[201] GDPR, art. 7(4); *see also* A29WP Consent Guidelines at 8.
[202] A29WP Consent Guidelines at 8.
[203] *Id.* at 9.
[204] *Id.*
[205] HIPAA regulations, 45 C.F.R. § 164.508(c)(2)(i-iii).
[206]GDPR, art. 7(3).
[207] *Id.*
[208] CCPA § 1798.125(a)(1).
[209] A29WP Consent Guidelines at 21.
[210] CCPA § 1798.120(a).
[211] *Id.*

Seventh, some existing regimes require **consent to changes** in data practices, suggesting that consent is dynamic and changes over time**:**

- Under COPPA, any changes to the collection, use, or disclosure, practices that the parent already consented to must be followed with a new notice to the parent, and a new request for consent.[212]
- Under the GDPR, using information for a different purpose from which it was gathered requires consent (if consent was the basis for processing).[213] Consent given by an individual must be in relation to "one or more specific" purposes, and the individual has the choice of whether to consent to each individual purpose.[214]

D. Incorporating Risk Management

The RFC rightly emphasizes the growing belief among users of digital products and services that they are "losing control over their personal information."[215] A 2014 PEW Research Center survey found that 91% of Americans agree that people have lost control over how personal information is collected and used by all kinds of entities. A year later, a Bain & Company survey found that consumers were often uncomfortable with how their data is used and shared and that over 66% of surveyed consumers feel that it should be illegal for companies to collect or use their data without getting prior consent. Even more disturbingly, a 2015 Annenberg School for Communication survey found that while 84% of Americans agree that they want to have control over what marketers can learn about them online, 65% have come to accept that they have little such control; this led the authors of the survey to conclude that people "have slid into resignation—a sense that that while they want control over their data world they will never achieve it."[216]

Thus, the RFC is right to treat trust as a core concern of U.S. privacy policy formation and to set NTIA the task of identifying "the best path toward protecting individual's privacy while fostering innovation," while at the same time noting that "risk-based flexibility" is the heart of its approach.[217]

---

[212] *Id.*

[213] GDPR, art. 7(1)

[214] A29WP Consent Guidelines at 11; *see also* GDPR, art. 6(1)(a).

[215] RFC, 83 Fed. Reg. at 48,600.

[216] Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up to Exploitation,* at 14 (June 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[217] RFC, 83 Fed. Reg. at 48,600; *see also* NIST SP 800-37:Rev. 2 (Draft), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Final Public Draft) (Oct. 2018), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft; Jody Blanke & Janine Hiller, *Smart Cities, Big Data, and the Resiliency of Privacy*, 68 HASTINGS L.J. 309, 348-59 (2017), http://www.hastingslawjournal.org/2017/02/10/smart-cities-big-data-and-the-resilience-of-privacy/.

The risk-based approach to privacy has several advantages including "focusing in on real priorities, providing interoperability and a common language across jurisdictions with different legal standards, and curing over-emphasis on notice and consent and collection alone."[218] Additionally, this approach allows organizations to develop scalable and proportionate responses to the varying levels of risk associated with specific practices of data collection and use in particular contexts, thereby avoiding one-size-fits-all regulatory solutions. This approach can result in efficient and effective outcomes if organizations heighten their compliance efforts whenever they engage in higher risk data practices.

However, in adopting a risk-based approach, it is crucial that regulators define privacy risk broadly enough to address the scope of significant and widely shared privacy concerns arising from citizens' unavoidably digital lives. The complex individual and societal risks associated with digitized personal data cannot be adequately characterized in terms of discrete downstream privacy harms, such as identity theft or reputational damage.

Moreover, the centralized structure of the digital economy poses enormous risks to many individuals in the face of a single breach. For example, a single incident recently compromised the personal data of over 50 million Facebook users. The privacy risks of today's digital society can be mitigated only proactively, collectively and upstream. In a "networked" world, information about one individual has implications for many. Individual efforts at self-help are increasingly ineffective. Because companies or the holders of the data are the most efficient risk-mitigators, they should be regulated, rather than relying on end users to somehow manage their own privacy protection.

Today's privacy harms encompass anxiety and resignation, the potential for being subjected to untraceable discrimination and manipulation, along with societal harms, such as loss of social trust and other costs associated with excessive surveillance, including chilling effects on free speech and associations and damage to democratic institutions. The risks are ubiquitous, and individual efforts to escape them are largely futile, as recognized, for example, in recent Supreme Court Fourth Amendment opinions joined by justices across the ideological spectrum.[219]

E. Making Accountability Effective

The RFC states that "organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems."[220] Accountability is central to existing data privacy regimes, which often rely heavily

---

[218] CENTRE FOR INFORMATION POLICY LEADERSHIP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (June 19, 2014), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf.

[219] *See* Carpenter, 138 S. Ct. 2206; Riley, 134 S. Ct. 2473.

[220] RFC, 83 Fed. Reg. at 48,602.

on cooperation with the private sector.[221] To both spur effective private participation and prevent regulatory capture, states must provide a backstop of accountability measures.[222]

Accountability can range from internal oversight to public transparency to third-party oversight to substantial state enforcement measures, including fines. Existing data privacy regimes have created a number of approaches to effective accountability.

First, some existing regimes encourage **internal accountability** within a company:

- Scholars have characterized the FTC's approach to data privacy as a form of collaborative governance that encourages, and in the context of consent decrees requires, companies to build up privacy compliance infrastructure, including through self-assessment and the appointment of privacy officers.[223]
- Under the GDPR's central principle of accountability, established in Article 5, companies are required to create internal compliance infrastructure and abide by significant reporting requirements.[224] In some cases, companies must put in place privacy officers.[225] In others, they must run impact assessments.[226] These internal changes attempt to make companies responsible—and internally accountable—for their own compliance. The GDPR's reporting requirements link internal accountability to regulatory accountability because reports must be provided to authorities.[227]
- The FCRA requires that companies put in place reasonable procedures for determining data accuracy.[228] These procedures can be understood as an attempt to create internal compliance infrastructure.

---

[221] *See, e.g.,* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 457–59 (2011); Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 380 (2011).

[222] *See* Margot E. Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA*, 94 DENVER UNIV. L. REV. 925, 938 (2016) (referring to this as a penalty default); *See* Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 Mich. Telecomm. & Tech. L. Rev. 1 (2016); W. Nicholson Price II, *Regulating Black Box Medicine*, 116 MICH. L. REV. 421, 465 (2017); Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 666 (2000) ("The background threat of regulation by an agency can provide the necessary motivation for effective and credible self-regulation"); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, MINN. L. REV, 112-113 (2004) (referring to David Dana's "contractarian regulation" and explaining that "command-and-control regulation is a precondition for contractarian regulation" as "actors that recognize the possibility of regulation… have an incentive to voluntarily reach a cooperative agreement").

[223] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

[224] GDPR, art. 33(1).

[225] GDPR, art. 37(1).

[226] GDPR, art. 35.

[227] GDPR, art. 33.

[228] FCRA, 15 U.S.C. § 602(b).

Second, some existing regimes establish **strong government enforcement regimes** housed with government regulators and often backed by substantial fines:

- The FTC is charged with enforcing Section 5's prohibitions on deceptive and unfair trade practices.[229]
- HIPAA, as amended by the Health Information Technology for Economic and Clinical Heath ("HITECH") Act, houses enforcement with the Department of Health and Human Services (HHS) and imposes a tiered penalty scheme that divides violations into various categories of culpability, given a set of factors.[230] HIPAA does not provide for a private right of action, but does allow state Attorneys General to pursue civil actions to enforce HIPAA Rules on behalf of state residents.[231]
- State Attorneys General currently enforce state consumer protection, data privacy, and data security laws, in addition to some federal laws.[232] Their enforcement toolkit includes litigation,[233] fines,[234] and establishing privacy governance through informal agreements with companies.[235] For example, as part of its settlement with state Attorneys General over collecting unsecured wireless network data through its Street View vehicles, Google paid a seven-million-dollar fine to states, in addition to signing an agreement requiring privacy awareness training and the development of related company policies and procedures.[236] The Indiana Attorney General's Office has, since 2002, negotiated settlements totaling over $22 million against telemarketers under federal and state Do Not

---

[229] 15 U.S.C. § 45(b)

[230] Health Information Technology for Economic and Clinical Heath ("HITECH") Act regulations, 78 Fed. Reg. 5566, 5583 ("Penalties under HIPAA are determined on a case-by-case basis as required by the statute at section 1176(a)(1) and the factors set forth at § 160.408. These factors include: (a) the nature and extent of the violation, (b) the nature and extent of the harm resulting from the violation, (c) the history of prior compliance with administrative simplification provisions, (d) the financial condition of the covered entity or business associate, and (e) such other matters as justice may require").

[231] HITECH, 78 Fed. Reg. at 5579.

[232] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME LAW REV. 747, 754 (describing sources of legislative authority for data privacy enforcement by state attorneys general, including UDAP laws), https://scholarship.law.nd.edu/ndlr/vol92/iss2/5/.

[233] *Id.* at 758.

[234] *Id.* at 785.

[235] *Id.* at 761-762.

[236] *Id.* at 785.

Call laws.[237] Uber famously recently negotiated a settlement of $148 million with all 50 states over its violation of state data security laws stemming from a 2016 data breach.[238]

- The CCPA will rely primarily on enforcement by the state Attorney General. The Attorney General may decide to bring a civil action in the name of the people of the State of California.[239] Similar to HIPAA, the adjudicating court must consider a set of factors in assessing statutory damages.[240]
- The Children's Online Privacy Protection Act (COPPA) places enforcement under the authority of the Federal Trade Commission and state Attorneys General.[241] A court can hold operators who violate COPPA liable for civil penalties of up to $41,484 per violation.[242]
- The GDPR enforces accountability through famously substantial fines. Under the GDPR the supervisory authority can impose fines of up to 4% of a company's global turnover of the preceding fiscal year for severe violations, or up to €20,000,000, whichever is higher.[243] Previously contemplated federal legislation established fines for knowing violations of up to $25,000,000, approximating the potential penalties under the GDPR.[244]

Third, some existing regimes create **a private cause of action**.

- The Fair Credit Reporting Act (FCRA) allows for consumers to bring suit against any person who willfully fails to comply with its requirements for any actual damages sustained by the consumer of not less than $100 and not more than $1,000,[245] as well as

---

[237] *Id.* at 777.

[238] Austin Carr, *Uber to Pay $148 Million in Settlement Over 2016 Data Breach* (Sept. 26, 2018), https://www.bloomberg.com/news/articles/2018-09-26/uber-to-pay-148-million-in-settlement-over-2016-data-breach.

[239] CCPA § 1798.155(b) ("In this case, a civil penalty of up to $2,500 for each violation and $7,500 may be imposed for each intentional violation").

[240] CCPA § 1798.150 (C)(2) ("the nature of the misconduct, the number of violations, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth").

[241] COPPA regulations, 16 C.F.R. § 312.9 ("A violation of COPPA is treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B).").

[242] *FTC Publishes Inflation-Adjusted Civil Penalty Amounts*, Federal Trade Commission, Press Release (Jan. 23, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts.

[243] GDPR, art. 83(5).

[244] Consumer Privacy Protection Act of 2015, Administration Discussion Draft, S.1158 § 107(a), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[245] FCRA, 15 U.S.C. § 1681n(a)(1)(A).

such punitive damages as the court may allow.[246] Additionally, a consumer may bring suit against any person who is negligent in failing to comply with any requirement for actual damages and, in the case of a successful action to enforce liability, the costs of the action together with reasonable attorney's fees.[247]

- Article 82(1) of the GDPR establishes a private cause of action; it allows any person the right to receive compensation for damage suffered.[248] In some ways broader than the FCRA, GDPR allows recovery for material or non-material damage as a result of infringement of the regulation, and is not limited to willful noncompliance or negligence.[249]
- The CCPA provides a private right of action in connection with unauthorized disclosure of personal information.[250] Under the CCPA, a consumer may also request injunctive or declaratory relief or any other relief the court deems proper.[251]

Finally, many existing regimes establish **transparency** requirements to trigger external oversight, including through both third-party audits and public transparency. Transparency is discussed at greater length in Section II(A).[252]

- The GDPR, for example, contemplates the use of third-party audits in establishing algorithmic accountability and fairness.[253]
- The Federal Trade Commission routinely requires audits (or third-party "assessments") in its settlements with companies.[254]

---

246 FCRA, 15 U.S.C. § 1681n(a)(2).
247 FCRA, 15 U.S.C. § 1681o.
248 GDPR, art. 82(1).
249 GDPR, art. 82(1).
250 CCPA § 1798.150(c) ("If a business fails to implement and maintain reasonable security procedures and practices that results in a data breach an individual may institute a civil action to recover damages of up to $750 per consumer per incident").
251 CCPA, § 1798.150(b); CCPA, § 1798.150(c).
252 *See* discussion, *supra* Part II.A.
253 See WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, pg. 20 onwards.
254 *See, e.g.*, Federal Trade Commission, *Frequently Requested Records*, https://www.ftc.gov/about-ftc/foia/frequently-requested-records/facebook; Federal Trade Commission, *In the Matter of Facebook, Inc.*, Federal Trade Commission, Docket No. C-4365 (Nov. 13, 2012), https://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf (requiring Facebook to "obtain initial and biennial assessments and reports ('Assessments') from a qualified, objective, independent third-party professional"). These assessments have, however, been critiqued as inadequate oversight compared to traditional audits. *See* Chris Hoofnagle, *Assessing the FTC's Privacy Assessments* (2016), https://ieeexplore.ieee.org/document/7448350/; *see also* Robert Gellman, *Lacking in Facts, Independence, and Credibility*: *The 2011 NAI Annual Compliance Report* (July 2012)

- California's Online Privacy Protection Act has since 2003 required online companies to have privacy policies that disclose the categories of personally identifiable information collected, among other things.[255]
- Enforcement actions by state Attorneys General have resulted in settlements requiring companies to both publicly disclose privacy practices and undergo annual privacy audits.[256]

III. Addressing Two High-Level Goals: FTC Enforcement and Harmonization

In closing, we address two of the proposed High-Level Goals for federal action: FTC Enforcement and Harmonization.[257] We respond to the call for proposed changes to the FTC's "resources, processes, and/or statutory authority" by calling for, among other things, both an expansion of FTC authority to include rulemaking, and greater transparency about FTC reasoning under its current authority. We respond to the call for harmonization by arguing against federal preemption of historic state efforts, noting that any discussion of harmonization must take care not to raise compliance costs for global companies by widening the gaps between U.S. and EU regimes.

A. FTC Authority

The RFC acknowledges the FTC's leading role in federal consumer privacy enforcement and specifically seeks comment on whether any changes are necessary regarding the FTC's "resources, processes, and/or statutory authority."[258] We suggest:

- That the FTC should be granted the authority to **promulgate rules** defining privacy-related unfair or deceptive practices;
- That the FTC should be granted the authority to **issue fines** in the first instance for violations of Section 5;
- That the FTC's **jurisdiction be clarified** to include communications companies and **be expanded** to include nonprofits;

(critiquing the audits conducted by the self-regulatory organization Network Advertising Initiative (NAI)), https://bobgellman.com/rgdocs/RG-NAI-2011.pdf.

[255] *See* CAL. BUS. & PROF. CODE § 22575 (West 2016), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=22575.&lawCode=BPC

[256] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME LAW REV. 747, 764; *see* Press Release, Office of the Att'y Gen. of Cal., Attorney General Lockyer Gains Enhanced Privacy Protections in Consumer Protection Cases (Aug. 28, 2002), https://oag.ca.gov/news/press-releases/attorney-general-lockyer-gains-enhanced-privacy-protections-consumer-protection.

[257] RFC, 83 Fed. Reg. at 48,602.

[258] *Id.* at 48,603.

- That the FTC should provide **greater transparency** about its reasoning in Section 5 settlements;
- That the FTC **assessment process** be improved;
- That the FTC address **data brokers**; and
- That the FTC be given more enforcement **resources**.

Several of these proposals are already included in pending legislation proposals.[259]

i. Rulemaking Authority

First, we believe that burdensome barriers to the FTC's authority to promulgate rules defining privacy-related unfair or deceptive practices should be removed so the agency can return to using conventional rulemaking procedures under the Administrative Procedures Act. In the 1980s, Congress limited the FTC's ability to engage in rule-making concerning deceptive and unfair practices under Section 5 by imposing burdensome procedural requirements.[260] As a result, the FTC tends to rely on strategic enforcement actions to achieve its regulatory goals, creating both uncertainty and opacity for consumers and for entities collecting, analyzing, or disclosing personal data. These procedural hurdles to standard rule-making should be removed.

Over the years, the FTC has developed considerable expertise in a range of privacy issues by holding workshops and/or issuing reports, studies, policy statements and several self-regulatory guidelines. It has issued recommendations on topics such as children's online privacy, data security, online behavioral advertising, facial recognition technologies, data brokers and mobile apps. Rule-making authority would permit the FTC to take better advantage of this expertise by issuing binding rules rather than voluntary guidelines, which have proven largely ineffective.

ii. Authority to Issue Fines

Second, in the absence of a privacy rule, the FTC lacks authority in most cases to impose a civil penalty when a company engages in unfair or deceptive practices.[261] As a result, most matters are resolved by consent decrees without civil penalties or other forms of monetary relief.[262] Currently, the FTC can issue fines only if companies later violate a consent decree or

---

[259] *E.g.*, Senator Ron Wyden, *Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy*, https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy (Nov. 1, 2018).
[260] Chris Jay Hoofnagle, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 65-66 (2016).
[261] 15 U.S.C. § 45(m)(1)(B).
[262] Federal Trade Commission, *Cases and Proceedings*, https://www.ftc.gov/enforcement/cases-proceedings (last visited Nov. 4, 2018).

for violations of specific statutory provisions such as in the context of COPPA.[263] It should be granted the authority to issue fines in the first instance for violations of Section 5.[264]

iii. Clarifying/Expanding Jurisdiction

Third, as the recent Ninth Circuit case *FTC v. AT&T Mobility* illustrates, there are both perceived and actual gaps in the FTC's jurisdiction.[265] The common carrier exception to the FTC's jurisdiction should be clarified to at least match the Ninth Circuit's interpretation.[266] The Ninth Circuit sitting en banc held that the common carrier exception applies only insofar as a common carrier engages in common carrier services; the FTC may thus regulate non-common-carrier practices by the same company.[267] Additionally, the FTC's jurisdiction should be expanded to include nonprofits, which can pose the same risks of data privacy harms but currently go largely unregulated.[268]

iv. Settlement Transparency

Fourth, we note that nearly all of FTC's Section 5 cases are resolved by settlements, not by litigation, resulting in a scarcity of published judicial decisions.[269] In view of the large number of settlements and their role in establishing "common law" rules through an incremental and bottom-up approach, the FTC should provide greater transparency about its reasoning.[270] For example, the FTC should:

- Issue more closing letters, particularly with respect to privacy-related allegations of unfair practices; and
- Provide more detail regarding its application of Section 5 to the facts at issue.[271]

---

263 15 U.S.C. § 45(m)(1)(B).
264 15 U.S.C. § 45(a)(l).
265 *See generally* FTC v. AT&T, 883 F.3d 848 (9th Cir. 2018), https://cdn.ca9.uscourts.gov/datastore/opinions/2018/02/26/15-16585.pdf.
266 15 U.S.C. § 45(a)(2) (excepting "common carriers subject to the Acts to regulate commerce").
267 FTC v. AT&T, 883 F.3d at 850 ("The phrase 'common carriers subject to the Acts to regulate commerce' thus provides immunity from FTC regulation only to the extent that a common carrier is engaging in common-carrier services.")
268 15 U.S.C. § 45(a)(1) (limiting FTC jurisdiction to "unfair or deceptive acts or practices in or affecting commerce")*; see also* California Dental Ass'n v. FTC, 526 U.S. 756 (1999)(finding that the FTC has jurisdiction over non-profits that operate for the profit of their for-profit members).
269 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, (2014). There are exceptions, of course, such as two recent decisions regarding the extent of FTC's authority to impose "reasonable" security requirements on firms under the unfairness prong of section 5. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); LabMD v. FTC, No. 16-16270 (11th Cir. June 6, 2018).
270 *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2294
271 *Id.*

v. Assessment Processes

Fifth, many FTC settlements require companies to obtain and submit initial and biennial "assessments" of their privacy and security programs. It is not clear that these assessments are of much help to the FTC in policing non-compliant companies.[272] Improvements to the assessment process could include:

- Requiring technical testing of system compliance;
- Specifying the standards that companies must meet in reviewing their programs;
- Making the assessment process more akin to an audit;
- Obtaining information from stakeholders outside the company as part of the FTC's review of assessments;
- Requiring disclosure of any material changes the company has made prior to the assessment, so that the assessment cannot merely assert that the company has been in compliance at all times; and
- Ensuring that assessments are more public and less redacted, so that interested technologists, academics, and plaintiff lawyers could help to ferret out non-compliance.[273]

vi. Data Brokers

Finally, the FTC should address contextual violations of privacy, even as applied to third parties. An example of policy action in this space is regulation of data brokers, who arbitrage data's value from one sector to another in ways that violate consumer's privacy expectations. The California CPA establishes a consumer right to opt out of having personal information sold from one organization to another. The FTC should explore this and other approaches to privacy issues arising from cross-context information flows.

B. Harmonization

The RFC states that the first high-level federal goal is to "[h]armonize the regulatory landscape."[274] While many industry actors have expressed concerns about state approaches to data privacy, we are not convinced that the burdens of state rules are as significant as they suggest. Moreover, we urge NTIA to recognize:

- That states have strong historic interests in regulating both privacy and security, and have been enacting and enforcing increasingly protective policies that we caution the federal government not to undermine; and

---

[272] Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE SECURITY & PRIVACY 58–64 (Mar/Apr. 2016).

[273] *Id.*

[274] RFC, 83 Fed. Reg. at 48,602.

- That the international landscape has seen upward harmonization of data privacy laws, such that a lower federal baseline will exacerbate compliance costs for global companies rather than lower them.

States have been important "laboratories for innovations in information privacy law."[275] For example, states were the first to impose data breach notifications, later copied in data protection laws around the world.[276] Both Massachusetts and Oregon have enacted omnibus data security laws, in the absence of federal protection.[277]

Moreover, existing federal privacy laws often serve as a protective floor for privacy regulation, rather than preempting growing state efforts and competencies in this area. HIPAA, for example, is a floor for health privacy regulation.[278] The Genetic Information Nondiscrimination Act (GINA) also serves as a floor, not a ceiling.[279] Federal laws have historically been careful to leave ample space for state actions. For example, while FCRA preempts some causes of action on the state level, it nonetheless allows states to regulate identity theft.[280]

Leaving states space to build on federal standards, rather than preempting them, has long been central to U.S. data privacy policy. It has allowed states to both experiment with policy and address the real concerns of their citizens. It has also deployed much-needed added resources towards these issues, beyond those of the federal government. Many state Attorneys General now address data privacy and security as issues of consumer protection, following in the footsteps of the FTC.[281] Preempting both these protections and these resources will set U.S. data policy back decades.

We therefore oppose wholesale preemption of state privacy laws and enforcement. NTIA should acknowledge that states have been the historic regulators of privacy in this country, starting with the privacy torts of intrusion upon seclusion, public disclosure of private fact, appropriation, and false light.[282] Rather than pushing states out of the policy picture, NTIA

---

[275] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 916 (2009).
[276] *Id.* at 917; *see also* Sen. Bill 1386, (Cal. 2002); A29WP: A29 WP, GUIDELINES ON PERSONAL DATA BREACH NOTIFICATION UNDER REGULATION,18/EN. WP250, ("A29WP Data Breach Notifications Guidelines") (Feb. 6, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
[277] *See* 201 CMR 17.00 (Mass.), https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf; Assem. Bill 1551, OR 646A.622., (Ore. 2018), https://olis.leg.state.or.us/liz/2018R1/Downloads/MeasureDocument/SB1551/Enrolled
[278] HIPAA regulations, 45 C.F.R. § 160.203 (2002).
[279] Genetic Information Nondiscrimination Act ("GINA"), 42 U.S.C. § 2(5), https://www.eeoc.gov/laws/statutes/gina.cfm.
[280] FCRA, 15 U.S.C. § 1681t(a).
[281] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME LAW REV. 747, https://scholarship.law.nd.edu/ndlr/vol92/iss2/5/.
[282] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 391-92 (1960).

should consider a cooperative federal-state approach that better recognizes the reality of strong state regulatory capacities in this space.

Second, any discussion of harmonization must recognize that the rest of the world is now harmonizing upwards of current U.S. data privacy law, towards the EU's GDPR.[283] It would be disingenuous and unhelpful to argue that harmonizing U.S. law will lower regulatory compliance costs, while in fact it may heighten gaps between U.S. protections and those set by the rest of the world.

Creating a larger gap between U.S. and European data privacy law will threaten already at-risk legal regimes for transferring data between those parts of the world.[284] This will raise, not lower costs, for companies doing business around the globe.

In lowering U.S. data protection at a federal level, including by preempting state laws, NTIA risks significantly raising already high costs for companies that do business globally. Companies that do business in the EU, monitor people in the EU, or envisage offering goods and services to people in the EU, already face significant compliance costs in modifying their behavior to the standards set by the GDPR.[285] Companies that wish to transfer data out of the EU to the United States must deal with the GDPR's significant restrictions on transfers of data to third countries.[286] The GDPR allows data transfers to third countries under only a limited number of circumstances: subject to an adequacy determination, which in summary recognizes that a third country's protections for data match high EU standards;[287] or subject to one of a series of private measures such as standard contractual clauses or binding corporate rules.[288]

The United States has, historically, been able to negotiate exceptions to EU rules on data transfers. The Safe Harbor allowed companies to streamline compliance by self-certifying to a certain level of protection;[289] that regime was invalidated by the European Court of Justice in

---

[283] *See, e.g.,* Brazil's GDPR, Lei No. 13,709 de 14 de Agosto, Diário Oficial da União [D.O.U.] de 15.08.18 (Braz.) ("Lei Geral de Proteção de Dados Pessoais" or "LGPD")

[284] INT'L. TRADE ADMIN., *Privacy Shield Overview,* https://www.privacyshield.gov/Program-Overview.

[285] GDPR, art. 3 & recital 23-24.

[286] GDPR, arts. 44-50.

[287] GDPR, art. 45.

[288] GDPR, art. 46.

[289] *Safe Harbor Certification*, PRIVACY TRUST, https://www.privacytrust.com/guidance/safe_harbor.html. "U.S. companies can opt into the [privacy shield] program (I.e. self-certify) as long as they adhere to the 7 principles and 15 frequently asked questions."

2015.[290] As a replacement, the U.S. negotiated the Privacy Shield, which is now also facing significant challenges in EU courts.[291]

Crucially: the viability of the Privacy Shield is understood to depend not just on federal standards of protection but on state enforcement.[292] Expert testimony in the ongoing Privacy Shield case (known as Schrems II) emphasizes state AG enforcement, state private rights of action, and class action mechanisms.[293] If NTIA decides to support efforts to preempt state enforcement, it must be sure to set a high enough floor of federal protections so as not to further threaten the Privacy Shield and thus raise regulatory costs for already burdened companies.

On the other hand, if NTIA decides to treat federal privacy legislation as a floor, this would not only increase harmonization with global standards, it might significantly lower global compliance costs for companies, while also raising protections for U.S. citizens. Any discussion of harmonization must take into account not just state-federal dynamics, but federal-global dynamics as well.

---

[290] Schrems v. Data Protection Commissioner (C-362/14 EU:C:2015:650 (06 October 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

[291] Lee Matheson, *Understanding 'Schrems 2.0'*, IAPP (Oct. 3, 2017), https://iapp.org/news/a/understanding-schrems-2-0/.

[292] *The E.U.–U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, BLOOMBERG (Sept. 12, 2016) https://www.bna.com/euus-privacy-shield-n57982076824/ ("The EU-U.S. Privacy Shield framework is largely a creation of U.S. law and enforcement will likely occur primarily in the U.S.: Commerce will scrutinize submissions, handle challenges and possibly request information from organization that register. Also, the FTC is the primary enforcement authority for Privacy Shield violations. And, at least in principle, the FTC, State Attorneys General and private plaintiffs can bring actions on unfair competition, misrepresentation and breach of contract theories in connection with any compliance vehicles.").

[293] Peter Swire, *Individual Remedies in U.S. Privacy Law,* at 7-30, 37 (2016), https://www.alston.com/-/media/files/insights/publications/peter-swire-testimony-documents/chapter-7--individual-remedies-in-us-privacy-law.pdf?la=en.