Comments of

TechFreedom

National Telecommunications & Information Administration (NTIA)

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

Berin Szóka & James Dunstan[i]

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

Executive Summary

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

I. Introduction

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

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

---

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

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

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

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

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

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

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

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

---

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

[5] *Id.* at 3.

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

[7] *See infra* at 9.

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

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

II. How to Think about Privacy

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

A. A Vast, Sprawling & Diverse Continent of Concerns

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

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

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

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

Solove argues for privacy pragmatism:

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

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

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

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

B. The Limits of the Property Rights Analogy

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

---

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

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

[11] *Id.* at 1146.

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

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

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

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

---

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

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

[14] *Id*. at 1.

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

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

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

---

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

[16] *Id*. at 18.

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

III. NTIA's Proposed Principles in Context

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

A. Comparison to the 2012 Obama Framework

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

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

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

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

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

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

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

---

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

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

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

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

[22] 5 U.S.C. § 552a.

[23] 15 U.S.C. §§ 6801-6809.

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

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

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

---

[24] 15 U.S.C. § 1681 et seq.

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

[26] 5 U.S.C. § 552.

[27] 15 U.S.C. §§ 6501–6505.

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

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

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

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

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

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

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

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

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

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

[35] *Id*.

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

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

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

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

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

C. California's CCPA

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

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

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

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

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

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

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

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

[42] CCPA § 1798.175.

[43] *Id.* § 1798.194.

[44] *Id.* § 1798.140(o)(1)

[45] *Id.* § 1798.130(a).

[46] *Id.* § 1798.135(a)(1).

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

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

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

---

[47] *Id.* § 1798.135(a)(2).

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

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

[50] *Id.* § 1798.150.

[51] *Id.* § 1798.125(a)(1).

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

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

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

IV. The First Amendment

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

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

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

[54] Determann, *supra* note 41.

A. The First Amendment & Deception

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

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

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

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

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

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

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

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

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

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

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

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

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

B. The First Amendment & Unfairness

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

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

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

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

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

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

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

[57] *Id*.

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

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

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

C. The First Amendment and Privacy Regulation

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

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

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

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

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

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

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

---

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

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

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

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

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

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

V. An Administrative Law Framework for Privacy

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

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

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

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

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

A. An Evolutionary Approach to Law

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

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

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

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

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

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

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

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

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

B. Rules v. Standards

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

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

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

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

.

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

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

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

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

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

[69] *Id*. at 15.

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

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

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

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

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

C. Standards as the Basis for Analytical Rigor

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

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

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

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

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

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

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

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

[76] *Id*.

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

D. Deference & Judicial Review

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

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

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

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

McWane, 783 F.3d 825.

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

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

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

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

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

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

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

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

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

E. Burdens of Proof

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

F. Fair Notice

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

---

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

[90] 15 U.S.C. § 45(b).

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

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

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

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

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

---

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

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

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

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

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

G. Civil Penalties

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

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

---

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

[96] *See infra* at 33

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

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

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

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

---

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

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

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

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

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

VI. Enforcement

The RFC asks:

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

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

---

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

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

A. Federalism & Preemption

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

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

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

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

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

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

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

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

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

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

B. Private Right of Action

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

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

---

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

[105] *Id.* at 21.

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

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

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

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

VII. Specific Comments on Proposed Principles

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

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

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

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

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

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

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

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

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

As we noted:

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

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

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

---

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

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

[114] NTIA International Priorities at 8-9.

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

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

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

B. Principle #1: Transparency

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

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

---

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

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

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

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

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

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

C. Principle #2: Control

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

And finally:

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

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

[123] *Id.*

[124] *Id*.

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

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

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

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

---

[125] *Id.*

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

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

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

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

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

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

3. How the Commission Pleads Cases

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

E. Principle #4: Security

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

[129] *Id*. at 6.

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

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

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

1. Cost-Benefit Analysis.

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

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

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

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

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

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

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

2. Comparison to Industry Practice.

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

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

---

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

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

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

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

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

3. Causation

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

Section 5(n) currently requires that:

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

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

---

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

[137] 15 U.S.C. § 45(n).

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

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

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

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

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

[141] *Id*. at 1294.

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

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

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

The ALJ's decision put it best:

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

As our brief noted:

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

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

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

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

F. Principle #5: Access & Correction

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

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

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

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

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

---

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

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

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

G. Principle #6: Risk Management

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

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

H. Principle #7: Accountability

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

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

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

---

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

[147] *Id*.

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

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

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

---

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

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

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

VIII. A Privacy Law Modernization Commission

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

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

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

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

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

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

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

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

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

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

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

[152] *Id*. § 11053.

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

IX. Conclusion

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

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

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

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