Comments of

TechFreedom

Federal Trade Commission

FTC Hearing on Competition and Consumer Protection in the 21st Century: February 12-13, 2019

(December 21, 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.

Contents

I. Introduction

We commend the Federal Trade Commission (FTC) for holding this series of workshops, and this workshop in particular. We have been urging the Commission to seek public input in rethinking its approach to privacy in particular and consumer protection issues generally since 2012. We addressed many of the issues discussed herein, and other issues, in our recent comments to the National Telecommunications & Information Administration (NTIA) on their proposed privacy framework.[2] In particular, those comments sketch out an "Administrative Law Framework for Privacy."[3] We have previously addressed these and other issues in a series of related work, including:

- Berin Szóka, Graham Owens, & Jim Dunstan, *Hearings on Competition & Consumer Protection in the 21st Century* (June 2018), https://bit.ly/2R9TGZy;
- 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), https://bit.ly/2PVZvVy;
- Berin Szóka & Geoffrey A. Manne, *The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature* (May 2016), https://bit.ly/2R9TLfO;
- 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), https://bit.ly/2V2vzel.

In brief, we urge both the Commission and, indirectly, Congress, to consider taking seriously the analytical tools of unfairness and deception that have been the bedrock of the FTC's consumer protection work for decades, and to ground new legislation in those concepts. The FTC's current case-by-case, *ex post* approach to enforcement, through injunctions and remedial relief, are the only appropriate way to deal with the enforcement of broad standards, including both those contained in Section 5 and any new standards that might refine, supplement, or replace Section 5 in the areas of privacy and data security. Rules should be lim-

[2] Comments of TechFreedom, In the Matter of Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01 (Nov. 9, 2018) [hereinafter NTIA Consumer Privacy Comments], https://www.ntia.doc.gov/files/ntia/publications/techfreedom_ntia_comments_on_privacy_framework_-_11.18.pdf.

[3] *Id*. at 21-35.

ited to clearly understood, real, rather theoretical, problems and clearly harmful conduct rather than the kind of hard trade-offs that many "privacy" problems concern, and civil penalties should be limited to the enforcement of such rules.

Above all, the Commission should keep in mind that many of the questions posed today in the realm of privacy and data security are relevant to today only—technology will change, the players will change, and notions of privacy and security are equally likely to change. Privacy approaches that target particular companies may in practice merely stratify and entrench them as the current, and future leaders, of technology. This would be a huge mistake, and we must do everything we can to foster disruptive technologies that advance the state of the art and benefit humanity, rather than stop change in an effort to perfectly regulate the Internet of today.

II. Should the FTC have additional tools, such as the authority to seek civil penalties?

Understanding the proper scope of civil penalties and rulemaking authority is, we believe, the single most important aspect of any legislation governing privacy, data security, or generally transforming the FTC's approach to consumer protection.

The Commission has been through these issues before. In December 2009, the House passed Rep. Barney Frank's "Wall Street Reform and Consumer Protection Act of 2009" (H.R. 4173)—the "Frank" half of the now famous "Dodd-Frank" legislation passed by both chambers and signed by President Obama in 2010.[4] The House version of the bill would have given the FTC across-the-board authority to seek civil penalties for any act or practice the FTC deemed unfair or deceptive under Section 5 of the FTC Act. In addition, the House bill would have removed procedural safeguards imposed on FTC rulemaking in 1980 and allowed the FTC to prosecute those who aided and abetted violations of Section 5. These provisions were ultimately not included in the final version of the bill. Now, both ideas have reemerged.

A. Civil Penalties

Recently, the idea of "civil penalty authority" has been conflated with a very different idea: giving the FTC the authority to enforce not Section 5 but specific *regulations* with civil penalties. Indeed, Congress' practice since 1980 has been to pair narrow FTC authority to issue

[4] Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. §§ 5301-5303 (2010), https://www.congress.gov/bill/111th-congress/house-bill/4173/actions.

regulations on a specific topic (such as children's privacy), with the authority to enforce those regulations with civil penalties.

In general, civil penalties are appropriate for the enforcement of clear rules, but not broad standards—whether those are the current standards of unfairness and deception, or new statutory standards, such as "reasonableness," "respect for context," *etc*.—for two reasons. First, to impose penalties on companies for failing to predict where the FTC will draw the line under vague, open-ended standards such as those of Section 5 would violate basic constitutional principles of Fair Notice (a requirement grounded in the Due Process clause of the Fifth and Fourteenth Amendments).[5] The greater the potential penalty at stake, the clearer the notice required—something that can be achieved to some degree through the promulgation of regulations (since regulations, after all, can include both standards and rules). Second, the very thing that makes civil penalties useful in some circumstances—deterrent effect—also makes them counter-productive in most circumstances. Penalties should be reserved for conduct that is clearly and overwhelmingly harmful; imposing penalties on companies that fail to predict where the Commission will draw the line on balancing tests will force companies to over-calibrate for the risk of liability, sacrificing many beneficial uses of data.

Across-the-board civil penalty authority remains a bad idea for the reasons explained by then Commissioner Bill Kovacic in his 2010 Congressional testimony, which proved pivotal in persuading the Senate to abandon this idea (contained in H.R. 4173, approved by the House):

> to the extent that UDAP cases do make their way in front of judges (despite the already strong incentive to settle them, which would likely be aggravated by the FTC's ability to impose civil penalties), the possibility of civil penalties may cause courts to construe the FTC's authority more narrowly than it otherwise would have, thus limiting the FTC's ability to protect consumers.[6]

---

[5] *See generally* Gerard Stegmaier & Wendell Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 3 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263037; *see also* Gus Hurwitz, *In Wyndham, the FTC won a battle but perhaps lost its data security war*, AM. ENTERPRISE INST. (Aug. 27, 2015), http://www.aei.org/publication/wyndham-ftc-won-battle-perhaps-lost-data-security-war/.

[6] *Financial Services and Products: The Role of the Federal Trade Commission In Protecting Consumers—Part II: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. 4-5 (2010) (Prepared statement of Hon. William E. Kovacic, Commissioner, Fed. Trade Comm'n, submitted by Hon. Roger F. Wicker, U.S. Senator) [hereinafter Kovacic Testimony], https://www.govinfo.gov/content/pkg/CHRG-111shrg57895/pdf/CHRG-111shrg57895.pdf.

Furthermore, Kovacic continued,

> if the FTC were granted civil penalty authority for consumer protection violations, another possibility is that the Commission might routinely challenge as unfair acts, under its consumer protection authority, conduct which might also be challenged under its antitrust authority as unfair methods of competition (as it did in *N-Data*). Thus, it might seek (routinely or otherwise) civil penalties for competition infringements. Here, also, Judicial fears about overdeterrence could induce courts to cramp the sensible development of doctrine.[7]

Kovacic concluded:

> Given these concerns, instead of across-the-board civil penalty authority, Congress may consider more targeted authority to seek civil penalties where restitution or disgorgement may not be appropriate or sufficient remedies. 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. What makes these cases distinguishable is that 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 the amount of restitution. In addition, disgorgement may be problematic. In data security cases, defendants may not have actually profited from their unlawful acts. The Commission has also found that in pretexting and spyware cases, the defendants' profits are often minor, and disgorgement would accordingly be an inadequate deterrent.[8]

This is a sensible way to think about how Congress should decide when civil penalty authority is appropriate for legislation targeted at specific problems. But giving the FTC's authority to seek civil penalties in *some* data security matters does not necessarily mean that *every* data security failure is an appropriate candidate for civil penalties—and this is even more true for "privacy," which consists of a far broader umbrella of related issues, involving even more difficult tradeoffs between consumer harms and benefits in the uses of data. In brief, we believe civil penalties should be targeted at enforcement of legal requirements that can not only be reduced to regulations promulgated through notice and comment, but also to rules, rather than broad standards such as "reasonableness" or "respect for context." Such standards, as we discuss below, are really only reformulations (appropriate or otherwise) of

[7] *Id*. at 5.

[8] *Id*. at 5-6.

unfairness and deception; applying civil penalties to them is problematic for many of the same reasons as to the unfairness and deception standards of Section 5.

While one can speak of the "enforcement" of rules, standards can only be "applied," not enforced—precisely because what the law requires depends on the unique facts of each case. Applying civil penalties to broad standards is problematic generally, but especially in matters of consumer protection related to the data privacy, Internet and other emerging technologies, for four specific reasons:

1. Almost by definition, tech companies do novel things, so there are no clear answers *ex ante* and the analysis necessarily involves tradeoffs that are likely to be un-understandable to regulators who often cannot understand the tradeoffs until much later. Imposing heavy liability on tech companies for failing to predict what the law will require would drive them to seek permission for their innovation—undermining the tradition of "permissionless innovation" that has made America the world leader in such services.[9]

2. The scale of such services would enable a determined regulator with civil penalty authority to seek enormous penalties by simply increasing the number of violations charged, whether by incident or day or user. Congress cannot easily constrain this discretion; even a relatively low maximum penalty threshold would enable arbitrarily high penalties through creative violation counting. To provide *some* meaningful limit, the new European General Data Protection Regulation (GDPR) caps civil penalties at either 2% or 4% of global turnover, depending on the category of violation.[10] Sen. Ron Wyden's (D-OR) Consumer Data Protection Act of 2018 would impose a single ceiling of 4% revenue.[11] In theory, these ceilings might prevent regulators from imposing even larger penalties by daisy-chaining multiple instances of a violation across a large number of users or a large number of days, or artificially charging as separate violations multiple instances of related conduct. In practice, these "ceilings" are likely to serve as penalty that will be expected by activists, politicians and the media, and thus force up the amount of penalties, even for relatively minor violations. In any event, the FTC would retain enormous leverage over regulated entities.

---

[9] *See* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2016), *available at* https://www.mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom.

[10] *See, e.g.,* European Union, *EU General Data Protection Regulation: Fines and Penalties* (last visited Dec. 20, 2018), https://www.gdpreu.org/compliance/fines-and-penalties/.

[11] Consumer Data Protection Act of 2018, S. 2188, 115th Cong. (2018), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

3. The FTC already has massive leverage over such companies even without the threat of civil penalties. As we have explained at length elsewhere, the FTC's astonishing track record of persuading very nearly 100% of the targets of its privacy and data security actions to settle illustrates the unique public relations sensitivity surrounding these topics. In theory, the possibility of civil penalties could drive encourage companies to litigate some cases, if the FTC is insistent on imposing civil penalties, but the FTC's ability to negotiate over the amount of civil penalties would also provide a powerful incentive for companies to settle.

4. Further compounding the dynamic by which these cases are resolved without judicial review would mean that regulators, not judges, would determine the course of consumer protection law on new technological frontiers. This has been our chief concern motivating all of our work on FTC process reform. This has been the chief concern motivating all of our work on FTC process reform.

For more detail on civil penalty authority, see our comments to the NTIA on their proposed privacy framework.[12]

B. Rulemaking Power

Much more attention has been paid to the issue of rewriting the FTC's current rulemaking power to remove the safeguards put in place in 1980 after the FTC's abuse of the powers Congress gave it in the Magnuson-Moss Act of 1975.[13] Jon Leibowitz, FTC chairman back in 2010, supported H.R. 4173, but attempted to reassure lawmakers that the FTC would use this power judiciously, as *Communications Daily* reported:

> The FTC would use expanded authority only where consumers suffer "significant harm," bad behavior is common in the industry, standards would improve practices and the expected burdens are "reasonable," Leibowitz said. "We'd be really stupid if we try to solve every problem in American society with a rule," he said, so the commission will use any new authority "very judiciously…." Where business practices and consumer expectations are "evolving," self-regulation is working and First Amendment issues are involved, the FTC would hold back, he said… [including] behavioral advertising and marketing to children. It would show

[12] *See* NTIA Consumer Privacy Comments, *supra* note 2, at 45-46.

[13] J. Howard Beales III, *The Federal Trade Commission's Use of Unfairness Authority: Its Rise, Fall, and Resurrection,* 22 J. PUB. POL'Y & MARKETING 192 (2003) [hereinafter Beales, *FTC's Unfairness Authority*] https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

> "enormously bad judgment to pursue those matters, Leibowitz said. "We do believe in self-regulation."[14]

In other words, as I noted at the time, "just trust us!"[15] The FTC's checkered history with rulemaking power in the 1970s provides good reason *not* to trust the FTC not to abuse broad power to make rules.[16] As Commissioner Kovacic noted in his testimony:

> While many other agencies do have the authority to issue rules following notice and comment procedures [of the APA], the Commission's rulemaking is unique due to the range of subject matter (unfair or deceptive acts or practices) and sectors (reaching broadly across the economy, except for specific carve-outs). Except where Congress has given the FTC a more focused mandate to address particular problems, beyond the FTC Act's broad prohibition of unfair or deceptive acts or practices, I believe that it is prudent to retain procedures beyond those encompassed in the APA.[17]

At that Senate hearing, Sen. Kay Bailey Hutchison (R-TX) provided an apt summary of how Congress had, in the past, considered the issue, and should do so in the future:

> In evaluating whether, and how, to change the scope and extent of FTC regulatory authority, I believe we must first ask whether there is a particular exigency, or area of consumer harm, that is so pervasive that the FTC's existing enforcement capabilities and rulemaking processes are not sufficient to address the issue. Second, if there is such an exigency, is the proposed legislative change broadly applied, resulting in greater regulatory burdens across a wide range of industries, or is it appropriately narrow to provide the FTC greater ability to develop rules and carry out enforcement actions directly relevant to that exigency. Third, we need to consider whether the FTC has sufficient personnel in key areas of its responsibility to carry out its enforcement and consumer protection mandates.[18]

---

[14] Berin Szóka, *FTC Chairman Leibowitz: Just Trust Us, We Won't Abuse Vast New Powers!*, The Technology Liberation Front (March 21, 2010), https://techliberation.com/2010/03/21/ftc-chairman-leibowitz-just-trust-us-we-wont-abuse-vast-new-powers/.

[15] *Id*.

[16] *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).

[17] Kovacic Testimony, *supra* note 6, at 4.

[18] *Financial Services and Products: The Role of the Federal Trade Commission in Protecting Consumers p. II: Hearing Before the Subcomm. On Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transp.,* 111th Cong. 4-5 (2010) (statement of Hon. Kay Bailey Hutchinson, U.S. Senator), https://www.govinfo.gov/content/pkg/CHRG-111shrg57895/html/CHRG-111shrg57895.htm.

C. Rules v. Standards in Regulation

Even where Congress decides to grant the FTC rulemaking power over a particular issue, the Commission is likely to wind up largely relying on standards rather than rules anyway — in which case, the question is really simply about (a) adapting the FTC's current, generally applicable standards of unfairness and deception into some other standards and (b) whether it is Congress or the FTC that does so. More specific standards may well be appropriate for certain areas, including data security and privacy. But the basic problem facing either Congress or the FTC will remain that summarized so aptly by the FTC's 1980 Unfairness Policy Statement:

> The present understanding of the unfairness standard is the result of an evolutionary process. ***The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. 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.'"[19]

To the extent that the Commission is enforcing standards of similar breadth and vagueness as unfairness and deception, the basic logic of the Commission's approach to these standards will still apply: The Commission should enforce them through its existing remedial and injunctive powers, rather than civil penalties.

D. Criminal Liability

In addition to civil penalties, some are now talking about including *criminal* penalties in data security and privacy legislation. Sen. Wyden's Consumer Data Protection Act would also allow the FTC to seek "10-20 year criminal penalties for senior executives."[20] This notion of

---

[19] Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n, *et al*. to the Hon. Wendell H. Ford, Chairman, Consumer Subcomm., Comm. On Commerce, Science, & Transp., U.S. Senate, and the Hon. John. C. Danforth, Ranking Member, Consumer Subcomm., Comm. on Commerce, Science, & Transp., U.S. Senate (Dec. 17, 1980) [hereinafter FTC 1980 Unfairness Policy Statement], *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[20] Press Release, Hon. Ron Wyden, U.S. Senator, Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy; *see also* Consumer Data Protection Act of 2018, *supra* note 11.

imposing criminal liability for privacy violations has attracted particular attention. It would greatly magnify the concerns discussed above regarding civil penalties.

To pass constitutional muster, criminal penalties would likely have to be limited to the enforcement of clear rules issued through regulations, not standards (whether in regulation or statute). As a policy matter, criminal penalties would be appropriate only in extremely narrow circumstances: the knowing violation of some rule where severe harm is extremely likely on a scale so massive that the FTC's current remedies would prove inadequate. It is difficult to conceive of what such a targeted rule would be.

Sen. Wyden's bill would impose criminal sanctions—up to ten years in prison and up to "$1,000,000 or 5 percent of the largest amount of annual compensation the person received during the previous 3-year period from the covered entity"—for executives who certify any of the statements required by his bill in an annual report to the FTC knowing that the "the statement does not comport with all the requirements set forth in this section."[21] Those annual reports would have to certify to compliance with all of the requirements the Commission could implement by rulemaking under Section 7(b) of the bill. Thus, Wyden's bill would effectively criminalize violations of the Commission's rules.

In theory, the knowledge standard should focus criminal penalties on knowingly false statements—*i.e.*, claims that a company is compliance with FTC rules that it is actually violating. In practice, however, this is likely to be extremely messy. As noted above, many privacy, data security, and other tech-related issues will be difficult to reduce to rules, given the complexity of the issues and the rapidly changing nature of the marketplace. This means that the FTC's regulations will likely be more standards than rules where it matters most. For example, Section 7 of Wyden's bill, authorizing the FTC to issue implementing regulations of the bill's substantive requirements, uses the word "reasonable" no fewer than thirteen times. Even those rule-like regulations the FTC could issue under this vague statutory language are likely to be difficult to jive with the reality of how companies collect, use, secure and share data—thus forcing companies to have to assess their compliance in something other than a simple yes/no fashion. Either way, if the FTC concludes that a company's practices were not "reasonable" after the fact, or that a company's interpretation of a rule was incorrect, corporate executives may be able to argue that they lacked the requisite knowledge to be held criminally liable. Yet the possibility of having to defend against criminal liability will likely nonetheless have a significant *in terrorem* effect over how corporate management operates.

Fear of such liability will prove a significant deterrent for individuals to join startups. Smaller companies will suffer most; it's one thing for an entrepreneur to take out a mortgage on the

[21] Consumer Data Protection Act of 2018, *supra* note 11, at 15.

family house to finance a startup, but quite another to risk jail time and a felony conviction. America's tech sector would never have gotten off the ground if failure meant not just bankruptcy but prison.

E. Other Reforms & Ensuring Judicial Review

For our full analysis of various institutional process reforms proposed for the FTC, see Berin Szóka's 2016 joint testimony with Geoffrey Manne.[22] Most of the reforms we propose are aimed at reducing the current perverse incentive for companies to settle not just most but effectively *all* FTC complaints against them, which prevents the courts from having the opportunity to develop doctrine, as contemplated by the FTC's Unfairness Policy Statement:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. 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***.'"[23]

At a minimum, Congress and the FTC should avoid making the current dynamic even worse, as broad civil penalty authority would do.

III. What are the tradeoffs between *ex ante* regulatory and *ex post* enforcement approaches to privacy protection?

In general, the current approach is the right one: enforce generally applicable standards *ex post* with injunctive and remedial relief, and craft *ex ante* rules for resolving issues where the right answer is reasonably clear *ex ante*. Rules have the advantage of providing greater clarity to affected parties and ensuring that regulated parties (or at least their counsel) are made aware of the rule through publication in the Federal Register.

---

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

[23] *1980 Unfairness Policy Statement*, *supra* note 19 (emphasis added).

On the other hand, as noted above, it will be difficult, if not impossible, to resolve the hardest issues raised by technological change through *ex ante* rules, for the same reason Congress identified in the Unfairness Policy Statement: neither Congress nor the FTC can foresee all bad practices. Moreover, neither can possibly predict how to resolve ambiguous cases, where a practice may cause harm as well as benefit.

The advantages of an ex post include:

1. Consumer injury will be far clearer after the fact than before it;

2. The way the law handles hard problems of trade-offs is best developed on the facts of cases; and

3. Innovation is most compatible with an approach that does not attempt to prescribe an unknown (and often unknowable) future.

IV. How should First Amendment norms be weighed against privacy values when developing a legal framework?

We have written elsewhere about the First Amendment problems raised by regulations of the collection, use and sharing of data—as well as why the FTC's enforcement of its existing unfairness and deception power has avoided such problems.[24] Law Professor Jack Balkin has done an admirable job of summarizing such problems, and proposes that "many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users."[25] Balkin's framework could be helpful in conceptualizing ways to defend privacy regulation from First Amendment challenges, but as a practical matter, he offers little useful guidance about what legislation should look like. He concludes:

> Because personal data is a key source of wealth in the digital economy, information fiduciaries should be able to monetize some uses of personal data, and our reasonable expectations of trust must factor that expectation into account. What information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm.[26]

[24] *See* NTIA Consumer Privacy Comments, *supra* note 2, at 14-20.

[25] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016), https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

[26] *Id*. at 1227.

On a high level, this sounds reasonable. But it does not answer the critical questions. What does "unexpected" mean beyond what deception (including material omission) already requires? What does "disadvantage" mean beyond what unfairness already considers substantial injury? And most critically, what would constitute an "important social norm?" That sounds exactly like divination of what constitutes a violation of public policy—exactly what got the FTC into such hot water with Congress that the agency was forced to abandon such open-ended inquiry in the 1980 Unfairness Policy Statement.[27]

Law professor Jane Yakowitz offers a useful critique:

> A careless reader of Information Fiduciaries could come away thinking that the government can impose many more duties of confidentiality than it currently does without significant First Amendment interference. Parts of the Article encourage this reading by presenting the fiduciary relationship as a solution to generic privacy problems and by suggesting that any service provider who handles personal information might be characterized as a fiduciary
>
> …
>
> But any attempt to harness the power of fiduciary relationships in order to achieve broad privacy policy runs into an unavoidable problem: it violates the cardinal rule of content-neutrality. Balkin's "central point is that certain kinds of information constitute matters of private concern not because of their content, but because of the social relationships that produce them." If the regulated social relationship is defined by assessing the sensitivity of the information that is exchanged, then the social relationship merely serves as a stalking horse for speech.
>
> Given this problem, it is not surprising that Balkin's concrete formulation of an information fiduciary is rather narrow — too narrow, it seems to me — to contain Netflix, Amazon, and most other web services. According to Balkin, a company will not become an information fiduciary unless it takes active steps to induce trust; specifically, to reassure consumers that it will not disclose or misuse personal information. And even then, a company will still only be a fiduciary if these assurances of trust are consistent with social norms; that is, with the actual and reasonable beliefs of consumers. Most popular services collecting potentially sensitive data fall outside this definition. Netflix and Amazon attained their market power by studying and repurposing user data. The disclosure of personal information is the *raison d'etre* for Facebook and OkCupid, and the latter makes transparent, unapologetic use of personal data to generate research reports. Even email providers and search engines could make non-spurious arguments that they fall outside this definition (though the case for fiduciary treatment of these

[27] *See* Beales, *FTC's Unfairness Authority*, *supra* note 13.

seems far stronger since, like doctors and lawyers, they perform critical services for which candid, trusting relationships may have positive externalities on the rest of society).[28]

In short, Congress faces hard questions surrounding the First Amendment and its application to the use of data, however that use is framed. The best thing the Commission could do in informing Congress would be to hold a workshop specifically focused on First Amendment issues.

V. Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

Privacy protection currently depends on concepts of unfairness and deception—and should remain so. "Sensitivity" may be a useful shorthand for distilling and blending these concepts, but it should not be a substitute for the analysis required by either. If anything, the Commission should focus more clearly on uses of data, rather than kinds of data, and more clearly distinguish between *per se* harmful *uses* of data (which should always be prohibited) and sensitive uses of data (whose use requires special protections, such as opt-in from consumers).[29]

The Commission's 2012 Report appears, implicitly, to rely on unfairness in concluding that comments filed with the Commission "reflect a general consensus that information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data is sensitive."[30] Section 5(n) bars the Commission from making breezy assertions about public policy as a substitute for actual analysis of consumer injury, countervailing benefit, and reasonable avoidability by consumers.[31] Nonetheless, much of this list likely does reflect actual consumer injury.

The Commission deserves credit for declining in 2012 to expand the definition of *per se* sensitive information beyond this list, even while noting that "some commenters suggested that

---

[28] Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV 1941, 1950-51 (2016), https://lawreview.law.ucdavis.edu/issues/49/5/Response/49-5_Bambauer.pdf.

[29] *See infra* page 28.

[30] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS 58 (March 2012) [hereinafter FTC Privacy Report], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[31] 15 U.S.C. § 45(n).

information related to race, religious beliefs, ethnicity, or sexual orientation, as well as biometric and genetic data, constitute sensitive data."[32] The Commission also rejected arguments that "consumers' online communications or reading and viewing habits" should be considered sensitive, noting that "the inherent subjectivity of the question and …. the effects on market research if the definition of sensitive data is construed too broadly."[33]

Unfortunately, the Commission's list was not grounded in actual injury analysis. It also suffers from a lack of specificity. The Data Care Act of 2018, introduced by Sen. Brian Schatz (D-HI) provides a more specific list, including a variety of unique identifiers and access credentials; importantly, the bill breaks down "financial information" concretely: "a financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to a financial account of an individual."[34] This is an appropriate distillation of "financial information" into a clear list of private information whose disclosure could result in very tangible economic harms to consumers — most notably, through unauthorized access to their accounts, unauthorized charges, or, potentially, credit applications in their name.

But note what the bill does *not* include: any broad catch-all language about information that merely relates, in some broad way, to finance — such as, for example, search queries related to loans. This is just as it should be: special regulatory treatment *should* be reserved for categories of information that are both clearly definable and clearly connected to consumer injury. *Per se* rules, in general, are appropriate only when *both* conditions are met.

By contrast, the broad category of "health" information used in both the 2012 Report and the Schatz bill illustrates the problem both with a lack of specificity and with a failure to ground the Commission's analysis in the analytical toolkit of unfairness. The Data Care Act gets only somewhat more specific than the FTC report, defining as "sensitive" the following:[35] The Data Care Act gets only somewhat more specific than the FTC report, defining as "sensitive" the following:

> Information that relates to—
>
> (i) the past, present, or future physical or mental health or condition of an individual; or

[32] FTC Privacy Report, *supra* note 30, at 57.

[33] *Id*.

[34] Data Care Act of 2018, S. 3744, 115th Cong., https://www.congress.gov/bill/115th-congress/senate-bill/3744.

[35] *Id*.

(ii) the provision of health care to an individual;[36]

But what constitutes a "health condition?" If read expansively, this language could subsume a huge swathe of information, including fitness or diet content or apps, and news articles about the rise in "Trump Anxiety Disorder," or a Facebook post that claims that if the Senate confirms a certain judge, the poster will "blow my brains out" — categories of information where the potential for consumer harm is radically less than what would be associated with, say, medical treatment. Such lack of clarity about the scope of such a category illustrates just how far the Commission's definition of what is "sensitive" could stray from actual injury to consumers.

At a minimum, any legislation attempting to handle this issue should operationalize the 2012 Privacy Report's recognition that,

> risks to consumers may not justify the potential burdens on general audience businesses that incidentally collect and use sensitive information. For example, the Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases. Thus, if Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice. However, if a health website is designed to target people with particular medical conditions, that site should seek affirmative express consent when marketing to consumers.[37]

In limited circumstances, the analytical toolkit of deception, rather than unfairness, may serve as adequate grounds for understanding what "sensitive" information is. That is, the Commission may in some cases be justified in treating as sensitive that information which is material to consumer decision-making. The clearest example of such a category is previously private information, the other category mentioned by the 2012 Report. This may well be the *only* category of information that could arguably be treated as sensitive without evidence of harm because doing so ensures that companies cannot change the terms of a deal unilaterally. That is, if consumers agree to participate in a service on the assumption that certain information will be kept private, companies should not be able to make that information public without consent.

But the concept of deception was not intended to circumvent the concept of harm, which remains the focus of the FTC act; indeed, one can think of deception as a shorthand type of

[36] *Id*.

[37] FTC Privacy Report, *supra* note 30, at 47-48.

unfairness analysis where materiality stands as a proxy for substantial injury and where there are no benefits to consumers or competition.[38]

The Save Data Act provides a more precise, clearer, and appropriate version of the Commission's broad discussion of how to deal with the "unexpected revelation of previously private information." The 2012 Report said this:

> The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. **These harms may include the unexpected revelation of previously private information, including both sensitive information** (e.g., health information, precise geolocation information) **and less sensitive information** (e.g., purchase history, employment history) to unauthorized third parties. As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz. The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful. Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[39]

The Data Care Act defines as sensitive information only the "the nonpublic communications or other nonpublic user-created content of an individual."[40] We agree that this is a better formulation of the concept, precisely because it more closely corresponds to information that is likely to be material to consumer choice.

VI. Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?

Of course, consumers are heterogenous and consumer protection should reflect the diversity of their preferences. But what some users experience as harms, other users experience as benefits. Thus, Unfairness focuses on substantial injuries, which are experienced as such by

[38] *See* NTIA Consumer Privacy Comments, *supra* note 2.

[39] FTC Privacy Report, *supra* note 30, at 8.

[40] Data Care Act of 2018, *supra* note 34.

most users — and requires assessing countervailing benefits, which might be experienced by some users but not others. Deception provides another way to address heterogenous preferences:

> If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group.[41]

On a high level, this is the right analytical approach. In fact, this sentence combines two different but overlapping approaches. In general, the Commission will be on sounder ground in focused on the second part ("is directed to") because it will generally be easier to see consumer preferences reflected in the mirror of how content/service producers market their offerings to those preferences than to try to assess the states preferences of a group. Thus, for example, the Children's Online Privacy Protection Act (COPPA) can be understood as a statutory codification of this approach with respect to children under 13, since COPPA's definition of covered services hinges in critical part on the same "directed to" analysis.[42] One can imagine the FTC doing something very similar case-by-case had Congress never enacted COPPA, and the FTC could well do the same thing today for sites, services or devices directed to teens or, say, the elderly.

The FTC's recent report on "Protecting Older Consumers" illustrates how the "affects" prong can heavily overlap with, or supplement, the "directed primarily to" prong of the analysis contemplated by the Deception Policy Statement. After providing a list of illustrative enforcement actions, the Commission notes:

> This list includes cases involving student loan debt management schemes and violations of children's privacy laws. The perpetrators of such schemes ***may not typically target older adults***, but the cases are listed because they involve large and diverse groups of consumers. The ***affected consumers*** are likely to include an older adult paying off student debt for him or herself or for an adult child, or an older parent or grandparent caring for children who go online and wish to protect their privacy.[43]

---

[41] *See* Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to the Honorable John D. Dingell, Chairman, Comm. on Energy & Commerce, U.S. House of Representatives (Oct. 14, 1983) [hereinafter FTC 1983 Policy Statement on Deception], *appended to* Clifford Assocs., Inc., 103 F.T.C. 110 app. at 174 (1984); https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[42] 15 U.S.C. § 6501(4)(B).

[43] FED. TRADE COMM'N, PROTECTING OLDER CONSUMERS: A REPORT TO CONGRESS, 12-13, note 39 (Oct. 18, 2018), https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2017-2018-report-congress-federal-trade-commission/protecting_older_consumers_-_ftc_report_10-18-18.pdf.

The Commission must also take into account the real-world impact if wide-spread opt-in requirements were enacted and users of free services suddenly decided to refuse to opt-in to allowing data collection. The amount of valid data across the Internet would be diminished, the value of that data would decrease rapidly, and the ability of providers to continue to offer free services would be hampered. CCPA's response that providers cannot withhold services to those who do not opt-in to a provider's data policy may likely wake up in the near future to find that that service provider no longer exists or is now charging to provide a previously free service.

VII. Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?

No. But this is not really the question. The Commission has always protected consumers against non-market-based harms through its deception powers, which focus on materiality rather than the nature of harm: so long as consumers would have chosen differently but for the misstatement or omission, the practice can be deceptive. Deception should remain the Commission's analytical first line of defense in dealing with non-market-based harms.

The Commission's 1980 Unfairness Policy Statement does not rule out the application of unfairness to non-market-based harms:

> 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.[44]

In other words, the real question is not about the nature of the harm, but about the nature of the *evidence* required to show that the harm is substantial. The less clear the evidence available that a certain kind of "harmful" practice actually injures consumers, the more the decision of how to treat that "harm" should be left to Congress to decide.

[44] FTC 1980 Unfairness Policy Statement, *supra* note 19 (emphasis added).

VIII. Where should interventions be focused? What interventions are appropriate?

The longstanding concepts of unfairness and deception provide the clearest answers to this question. They should guide Congress even as it considers expanding upon these concepts in new statutory authority for the FTC.

The Commission should also be cognizant of, and seek guidance from, the current NIST Privacy Framework process. Important principles are being worked out by the engineering "side" of the government—those who understand the actual workings of how data are processed across the Internet, and where and when control of data may change hands. It is becoming evident that concepts such as "data processors" and "data controllers" as described in the GDPR are highly oversimplifications that may well result in significant unintended consequences. Put another way, before the Commission considers were to put the intervention "toll booths," a fuller understanding of the road system (*e.g.*, the actual workings of the Internet as utilized by those collecting, processing and sharing data) is required. We are hopeful that the NIST process will produce a workable "roadmap" of the ecosystem.

IX. How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?

The FTC's existing authority allows it to, under some circumstances, require both (1) notification to users when third parties misuse data, including by transferring it to fourth parties without authorization and also (2) the effective assertion of control by the first party over what third parties (and potentially, unauthorized fourth parties as well) do with that data, including by audits. We explored the potential use of the FTC's deception and unfairness authority in a letter we sent to Congressional leaders in April 2018, regarding Facebook's mishandling of the Cambridge Analytica. We conclude that (1) failure to notify Facebook users of the breach likely constituted a material omission, since many consumers would have made different choices about whether to user, or continue using, the site and (2) Facebook might have committed an unfair trade practice by failing to stop misuse of the relevant data, especially by failing to verify that this data had actually been deleted, as Global Science Research

had claimed, by insisting on an audit of GSR as well as Cambridge Analytica and SCL Elections (the two companies to which GSR had transferred that data).[45]

On the latter point, our letter—written in the days after the Cambridge Analytica scandal broke—failed to address one vital issue: the distinction between data that had previously been public and that which had previously been private (a specific category of sensitive information discussed above[46]). We quoted the Commission's 2012 Privacy Report as follows:

> The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. **These harms may include the unexpected revelation of previously private information**, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties.[47]

It now appears that, in general, the information accessed by Cambridge Analytica was, in general, previously public information: the names, birthdays and profile pictures of their friends (which was visible on Facebook even to people who were not their friends). While the ability to access this information *en masse* is troubling, and scraping such information in violation of Facebook's rules may well have raised other legal problems, it cannot be considered the "unexpected revelation of previously private information" and therefore a privacy harm, at least as far as the logic of the FTC's 2012 Privacy Report went. While this distinction should also play some role in the FTC's analysis of the materiality of Facebook's failure to disclose the unauthorized accessing of this information, we do not believe the difference was dispositive because many consumers would likely have made different decisions about whether, and how much, to use Facebook if they had known of this unauthorized use. Importantly, the remedy for this form of legal liability was simple: Facebook could have avoided liability for deception by material omission simply by telling its users what had happened.

However, it also now appears that a small subset of users of the GSR app had also authorized the app to access their private messages, including not only their own private information but that of other users. As *Wired* reports, "Facebook says that a total of 1,500 people granted

---

[45] Letter from Berin Szóka, President, TechFreedom & Graham Owens, Legal Fellow, TechFreedom, to Hon. Charles Grassley, Chairman, Committee on the Judiciary, U.S. Senate, and Hon. Diane Feinstein, Ranking Member, Committee on the Judiciary, U.S. Senate, *et al.* (April 10, 2018), http://docs.techfreedom.org/TechFreedom_Congressional_Letter-Facebook_hearing_4-10-18.pdf.

[46] *See supra* note 37 and accompanying text.

[47] FTC Privacy Report, *supra* note 30, at 7.

This Is Your Digital Life permission, although the total number of people affected remains unknown. Anyone who messaged those 1,500 people—or received messages from those 1,500—on Facebook at the time would be potentially impacted."[48] The FTC could argue either (i) that Facebook had a duty to ensure that its third party partners did not transfer this private data to fourth parties, or to use it in ways that users did not expect based on the nature of the choice presented to them or (ii) Facebook should not have allowed third party apps to read the contents of user messages (if that is actually what happened), even with the consent of one party to these conversations.

X. What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?

Opt-in requirements will tend to benefit big, well-established companies, who are best positioned to get consumers to opt-in to the collection of data (and to accept overly broad EULAs or terms of service because of their existing relationships).[49] Similarly, the history of innovation in the Internet ecosystem suggests that the dominance of existing incumbents can only be broken by disruptive, not adaptive, innovation — in other words, by radically new and different ways of doing things, or doing things that were previously inconceivable. Such new entrants are likely to have the most difficult time explaining to consumers the value proposition of their services, and thus be most at jeopardy in an opt-in world. More pointedly, they will also struggle to convince regulators of the value of their services, and thus face greater legal liability across-the-board.

One might think that data minimization mandates (and legal incentives to de-identify data) would help well established companies over smaller rivals, because big companies have more data, but the opposite may well be true: if "Big Data," and the ability to derive insights from it, is the key to transforming existing markets, or creating entirely new markets, small companies are likely to be burdened disproportionately by legal requirements that make it difficult to assemble such data sets, and even more, by restrictions on the ability of existing companies to share data with third parties. Regulation that favors data sharing within first parties (the data collectors) over the sharing of data with third parties will inevitably disfavor creative partnerships between established companies with valuable data sets but that

[48] Issie Lapowsky, *Cambridge Analytica Could Have Also Accessed Private Facebook Messages,* WIRED (April 10, 2018), https://www.wired.com/story/cambridge-analytica-private-facebook-messages/.

[49] Nicklas Lundblad & Betsy Masiello, *Opt-In Dystopias,* 7 Script*ed* 1 (2010), https://www.scribd.com/document/30469167/Opt-in-Dystopias.

perhaps lack technological savvy and tech-savvy but data-poor startups. This, in turn, will favor tech-savvy, data-rich incumbents (essentially, "Big Tech") and encourage vertical integration.

XI. Do firms incur opportunity costs as a result of increased investments in privacy tools? If so, what are the tradeoffs between functionality, innovation, and security and privacy protections at the design level?

The direct costs of privacy tools, including the opportunity cost of those investments, may be the most visible "costs" of privacy regulation, but they are likely to be dwarfed by the indirect costs of regulation—essentially, the foregone value of data. Data minimization offers the clearest requirement, reducing the value of data held by businesses. But the same can be true for any restriction on how companies may collect, use or share data. The Commission's analysis of the tradeoffs inherent in privacy regulation must focus on these costs, not the more easily measured direct costs. Otherwise, the Commission's economists risk falling prey to the classic "street light effect":

> A policeman sees a drunk man searching for something under a streetlight and asks what the drunk has lost. He says he lost his keys and they both look under the streetlight together. After a few minutes the policeman asks if he is sure he lost them here, and the drunk replies, no, and that he lost them in the park. The policeman asks why he is searching here, and the drunk replies, "this is where the light is."[50]

XII. If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker? What is the best way to strike that balance and assess its efficacy?

There are no easy answers to this question, but treating this question as purely *sui generis* is clearly the wrong *way* to answer it. That is, consumers regularly purchase goods and services whose workings, or manufacturing processes, they do not understand; in many cases, it would be impossible for them to do so, or at least, highly impractical to try. Privacy concerns are not inherently different; they are merely harder to address. Consumers deserve to be

[50] David H. Freedman, Wrong: Why Experts Keep Failing Us. Little, Brown and Company (2010).

informed about aspects of the products they use that could harm them (unfairness) or that are material to their decision to buy the product. Not all information is material and requiring the provision of non-material information to the consumer will merely cloud their ability to make informed decisions. Using terms like "sensitive" cannot bypass the need to think carefully about materiality.

XIII. Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?

Stated preferences do not reflect real tradeoffs made under conditions of scarcity. I addressed this topic in a 2009 paper: *Privacy Polls v. Real-World Trade-Offs*.[51] Moreover, privacy polls attempt, in highly artificial ways, to reduce complex systems to short statements that are likely to be even less informative to consumers than are the privacy policies and other educational pieces by which companies attempt to disclose their own privacy practices. Of course, survey results are highly susceptible to framing. Even more sophisticated behavioral economics experiments will struggle to replicate the real-world conditions under which consumers make decisions about using services that benefit them.

XIV. Given rapidly evolving technology and risks, can concrete, regulated technological requirements – such as data de-identification – help sustainably manage risks to consumers? When is data de-identified? Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable? If not, are there alternatives?

The FTC's 2012 report defined de-identification as follows:

> 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, 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

[51] Berin Michael Szóka, *Privacy Polls v. Real-World Trade-Offs*, 5 Progress & Freedom Found. Progress Snapshot Paper 10 (Oct. 2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1502811.

> 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. Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data. The Commission encourages companies and researchers to continue innovating in the development and evaluation of new and better approaches to deidentification. FTC staff will continue to monitor and assess the state of the art in de-identification.[52]

Implementing a workable de-identification standard, however, is proving problematic. For example, in our comments filed in July in response to the NTIA's Request For Comments (RFC), we pointed out that the GDPR's implementation of de-identification set an almost insurmountable bar that effectively establishes a strict liability standard for data de-identification:

> 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.[53]

Specifically, while the GDPR defines anonymization (literal impossibility of deriving insights on a discreet individual), it does not define pseudonymization, as one commentator has explained:

> 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.[54]

---

[52] FTC Privacy Report, *supra* note 30, at 21 (internal citations omitted).

[53] Comments of TechFreedom, In the Matter International Internet Policy Priorities, Docket No. 180124068–8068–01, 45-46 (July 16, 2018) [hereinafter NTIA International Priorities Comments], https://www.ntia.doc.gov/files/ntia/publications/comments_of_techfreedom_re_ntia_noi.pdf.

[54] 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/.

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.[55]

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.

At the outset, we argue that civil penalties are an inappropriate tool for enforcing broad standards that require companies to weigh tradeoffs.[56] Whether data has been "reasonably de-identified" is the paradigmatic example of such a standard. Imposing civil penalties on companies that fail to predict whether the Commission will decide they have inadequately de-identified data will force them to be dramatically overly cautious, and to err on the side of collecting and retaining *more* information.

---

[55] NTIA Consumer Privacy Comments, *supra* note 2, at 8-9.

[56] *See supra* pages 4-8.

XV. What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?

We analyze Europe's GDPR and California's CCPA in our November NTIA comments.[57]

XVI. If the U.S. were to enact federal privacy legislation, what should such legislation look like? Should it be based on Fair Information Practice Principles? How might a comprehensive law based on Fair Information Practice Principles account for differences in uses of data and sensitivity of data?

The Consumer Privacy Protection Principles (CPPPs) proposed by law professor Fred Cate in 2006 remain the clearest shorthand for our preferred approach.[58] Most critical are Cate's first two principles:

> 1. **Prevention of Harm**—Data protection laws should regulate information flows when necessary to protect individuals from harmful uses of information. Like other consumer protection laws, data protection law should be designed to prevent tangible harms to individuals and to provide for appropriate recovery for those harms if they occur. Tangible harms are defined as damage to persons or property.
>
> a. **Focus on Use**—Data protections laws should target harmful uses of information, rather than mere possession, and should focus on collection only to prevent collection by dishonest or deceptive means. Individuals are less likely to be harmed by the mere collection, possession, or transfer of accurate information. Moreover, even information that could be used for harmful purposes may also have uses that are beneficial for the data subject, the data user, and society as well.
>
> b. **Proportionality**—Data protection should be proportional to the likelihood and severity of the possible harm(s).
>
> c. **Per Se Harmful Uses**—Where a use is always harmful (e.g., the use of personal information to commit fraud), the government should prohibit the use outright.

[57] *See* NTIA Consumer Privacy Comments, *supra* note 2.

[58] Fred H. Cate, *The Failure of Fair Information Practice Principles: Consumer Protection in the Age of the Information Economy* (2006), https://ssrn.com/abstract=1156972.

d. **Per Se Not Harmful Uses**—The government should not regulate uses that present no reasonable likelihood of harm.

We stipulate here that the FTC should continue to enforce its deception authority, even without clear proof of harm.

e. **Sensitive Uses**—Where a use of personal data is neither "per se harmful" nor "per se not harmful," the government may condition the use on obtaining the consent of the data subject(s). Such requirements should be reserved for uses of personal data:

i. that are reasonably and objectively thought to be intrusive, offensive, or otherwise invade personal privacy;

ii. where the intrusion, offense, or other objection is directly related to the use of personal data; and iii. where consent likely would be effective.

2. **Benefits Maximization**—Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and individual privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. Therefore, the goal of any privacy regime must be to balance the value of accessible personal information with the value of information privacy to maximize both individual and public benefits.

a. No data protection law should be enacted or enforced that does not in fact significantly serve the purpose for which it was enacted. Laws that are ineffective or that are enacted without a specific purpose run the risk of imposing costs without achieving benefits.

b. Data protection laws should not be enacted or enforced if they are substantially more burdensome or broader than necessary to serve that purpose. Such laws by definition impose costs in excess of the benefits they achieve. Similarly, some data protection laws, even if narrow and precise, may necessarily impose costs that exceed their benefits.

Any legislation should include the kind of structural reforms we have detailed in our past work on the FTC's investigative, enforcement, and settlement processes.

XVII. Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

No. States have no business regulating the inherently interstate—indeed, global—media that comprise Internet and Internet-enabled services. Inevitably, one state's regulatory framework will govern all Internet services, at least if that state is large enough to be indispensable (*e.g.*, California) and conflicts between inconsistent state laws will place regulated companies in increasingly difficult, if not impossible, positions.[59] No time is needed to assess their effects because they offend the most basic principles of Federalism. They should be preempted immediately.

XVIII. Short of a comprehensive law, are there other more specific laws that should be enacted?

There has long been wide consensus that federal breach notification legislation makes sense and giving the FTC rulemaking and civil penalty authority in this area is uncontroversial. Legislation to clarify the standards for data security could also be an improvement over the status quo; in particular, Congress could make clear that the assessment of the reasonableness of data security concerns the *processes* by which a company decides how to manage data security. Legislation could also be targeted at how companies ensure that data they provide to third parties is both secured and also used in a way consistent with user expectations throughout the supply chain, such as through audits and technical controls.

In addition, we have long supported expanding the FTC's jurisdiction to cover non-profits and common carriers. We have proposed several detailed reforms of the FTC's processes.[60]

---

[59] Graham Owens, *Federal Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail,* 56-87 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216665.

[60] *See* SZÓKA & MANNE, RESTORING CONGRESSIONAL OVERSIGHT, *supra* note 22.