MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

THE IMPORTANCE OF BALANCING PRIVACY WITH INNOVATION, CONSUMER BENEFITS, AND OTHER RIGHTS IN THE FTC'S APPROACH TO CONSUMER DATA PRIVACY

JENNIFER HUDDLESTON
Research Fellow, The Fourth Branch Project, Mercatus Center at George Mason University

Agency: Federal Trade Commission
Comment Period Opens: October 29, 2018
Comment Period Closes: May 31, 2019
Submitted: May 30, 2019
Docket No. FTC-2018-0098-0003

I welcome the opportunity to submit comments regarding the Federal Trade Commission's (FTC's) requests and recent hearings on 21st century consumer privacy and the accompanying questions on the topic. In my view, this topic and specifically the FTC's approach to addressing privacy concerns must balance any risks of harm with the benefits of innovation and data usage that many consumers also experience. Furthermore, privacy does not exist in a vacuum and the potential impact of favoring privacy over other rights such as freedom of speech must also be carefully considered. The questions asked by the FTC and the accompanying hearings indicate the agency desires to find an appropriate balance on these issues that will continue to enable future innovation.

While the FTC asks many important questions in this request, I plan to limit these comments to the following topics:

- The variation in consumer preferences regarding data privacy and the tradeoffs the agency should consider
- The FTC's approach to harm and the cautious considerations about expanding any definition to include nonmarket harm and the existing legal frameworks and FTC approach to addressing data privacy concerns
- The tradeoffs between ex ante and ex post regulation
- The potential friction between First Amendment rights and privacy regulations
- The consideration of any expanded FTC authority or additional privacy laws outside of a comprehensive proposal

For more information, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201

CONSUMER PREFERENCES AND DATA PRIVACY

Consumer preferences for data privacy differ dramatically depending on the nature of the data or the type of interaction.[1] The majority of Americans make pragmatic choices regarding data privacy and security by choosing better data security and more privacy-sensitive providers for transactions involving sensitive information such as financial data or health information.[2] They recognize that data is frequently used in modern information technology. Frequent users of social media or search engines generally understand to some degree that their information is being tracked, and even when they express a preference for not having their browsing tracked, they are generally unwilling to pay for opting out of such monitoring.[3] While this apparent disconnect is often termed the "privacy paradox," consumers do take steps that are consistent with varying levels of privacy preferences.

Ten to twenty percent of Americans would be considered "privacy unconcerned" and a third (or fewer) would be considered "privacy fundamentalists."[4] The remaining majority in the middle of these two positions takes a pragmatic approach that varies depending on the situation and data under consideration.[5] Given this range of preferences, individuals currently deploy a variety of tactics and use various market responses to address the usage or retention of data. Tens of millions of users have used Google's privacy checkup since it launched in 2015 to assess or reassess their current settings.[6] Similarly, according to 2018 Reuters polling data, the majority of Facebook users polled were aware of their privacy settings on the service.[7] More privacy-sensitive Americans are also utilizing various tools such as ad blockers or monitoring services.[8] In fact, a majority of internet users polled had taken basic steps such as clearing cookies or browsing history, and a sizeable number have enabled two-factor identification on select accounts or opted out of cookie usage as a result of their privacy preferences.[9]

These preferences can vary dramatically, and most Americans do not find themselves trapped by the data-driven websites; they choose to participate because they find those services beneficial. According to Zogby polling data conducted for NetChoice, 42 percent prefer targeted ads based on data collection to nontargeted ads.[10] Americans also find themselves willing and able to leave platforms they no longer find beneficial, with 43 percent of participants in the same survey saying they had left a social media platform at some point.[11] While only a small percentage chose to leave because of changes in a privacy policy,[12] consumers nonetheless make choices when it comes to data-driven services.

---

[1] *See, e.g.*, Pew Research Ctr., *The State of Privacy in Post-Snowden America*, FACT TANK, Sept. 21, 2016, https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[2] Alec Stapp, *Against Privacy Fundamentalism*, Niskanen Center, Nov. 19, 2018, https://niskanencenter.org/blog/against-privacy-fundamentalism-in-the-united-states/.

[3] *See* CALEB FULLER, HOW CONSUMERS VALUE DIGITAL PRIVACY: NEW SURVEY EVIDENCE (Feb. 2018).

[4] Stapp, *supra* note 2 (describing a series of survey and study results conducted by Alan Westin and others).

[5] *Id.*

[6] *See* Lauren Goode, *Google's New Privacy Dashboard Makes It Easier to See What Google Knows About You*, THE VERGE (Sept. 8, 2017, 12:30 PM), https://www.theverge.com/2017/9/8/16276000/google-dashboard-my-account-privacy-security-redesign.

[7] Reuters Poll Data: Social Media Usage Poll 05.03.2018 (May 3, 2018), http://fingfx.thomsonreuters.com/gfx/rngs/FACEBOOK-PRIVACY-POLL/010062SJ4QF/2018%20Reuters%20Tracking%20-%20Social%20Media%20Usage%205%203%202018.pdf.

[8] Remie Arena, *What Are Consumers Doing to Keep Their Personal Data, Well, Personal?*, EMARKETER, June 12, 2018, https://www.emarketer.com/content/what-are-consumers-doing-to-keep-their-personal-data-well-personal?ecid=NL1001.

[9] *See id.*

[10] *American Consumers Reject Backlash Against Tech*, NETCHOICE (last visited May 17, 2019), https://netchoice.org/american-consumers-reject-backlash-against-tech/.

[11] *See id.*

[12] *Id.*

Given this range in preferences, the FTC should be cautious about regulation that would unfairly favor a particular set of privacy preferences at the risk of losing the benefits that many Americans enjoy. Together with my colleagues Anne Hobson and Adam Thierer, I offered comments to the Consumer Product Safety Commission regarding cybersecurity and the internet of things, advising the agency to consider how education could play a role in empowering consumers to act according to their individual preferences.[13] Considering that consumers will make choices aligned with their preferences when they are concerned about and aware of potential risks, such as selecting more secure products or taking action that results in companies instigating voluntary recalls, greater weight should be placed on public education of best practices. These educational programs should inform users of security best practices when browsing online and using social media, such as regular checking and adjusting of privacy settings, clearing cookies or web history, and availing themselves of other existing options.[14] Rather than regulate a particular set of preferences regarding data privacy, the FTC should focus on allowing consumers to select the options most aligned with their preferences and should foster a robust and competitive market that is able to provide a wide range of options for consumers to choose from.

APPROACH TO HARM IN THE DATA PRIVACY CONTEXT

The FTC has addressed market-based harms that occur owing to data breach and consumer-welfare-harming data privacy issues. Now the FTC asks whether its enforcement should include nonmarket injuries such as embarrassment. I suggest that given the difficulty in identifying any objective standard, the FTC should avoid addressing such vague harms unless there is evidence of an objective and measurable impact on consumer welfare. An overly broad definition of harm could stifle innovation and many of the uses of data that consumers actually find beneficial owing to a subjective concern such as creepiness or embarrassment.[15]

In a previous comment filed with the FTC in 2017 regarding the question of informational injury, Chris Koopman, Adam Thierer, Andrea O'Sullivan, and I discussed the importance of avoiding a "theory of everything" when it comes to injury in the data privacy and data security context.[16] As we pointed out then, a broad definition of harm on these issues could undermine innovative use of data, in which the US companies have been leaders. Regulation based on such a broad definition would be impractical to enforce and tricky to comply with for companies in the information technology space and beyond.[17]

The tech sector in Europe is small and growing slowly compared to the American one. One potential explanation for this difference is regulation. European companies are weighed down by heavy regulation, while their American counterparts are free to innovate and introduce new products with minimal regulatory hurdles.[18] This difference has only become more pronounced since the enactment of the European Union's General Data Protection Regulation (GDPR) in May

[13] Adam Thierer, Jennifer Huddleston Skees & Anne Hobson, The Internet of Things and Consumer Product Hazards (2018).
[14] *See id.*
[15] *See* Adam Thierer, *On "Creepiness" as the Standard of Review in Privacy Debates*, Technology Liberation Front, Dec. 13, 2011, https://techliberation.com/2011/12/13/on-creepiness-as-the-standard-of-review-in-privacy-debates/.
[16] Christopher Koopman, Adam Thierer, Andrea Castillo O'Sullivan & Jennifer Huddleston Skees, Informational Injury in FTC Privacy and Data Security Cases (2017).
[17] *Id.*
[18] *Id.*

2018 as smaller players have continued to exit the market while larger players have gained market share and devoted substantial resources to compliance in order to continue operation in the market.[19] This response shows that a regulatory approach modeled after GDPR could result in tradeoffs including fewer choices for consumers and less competition from innovators. Yet competition is key for new companies to offer better data privacy and security options than current players.[20] Rather than attempting to define every possible noneconomic harm and provide redress, the FTC should stay the course and focus on the objective and clear examples of harm to consumer welfare when it comes to data privacy.

When it comes to drawing such lines regarding harm in data privacy, the FTC should not overstep its authority without clear direction. While the FTC has generally filled the role of data privacy regulator in the United States, it has not received express delegation over such matters from Congress beyond targeted areas such as children's online privacy.[21] Before establishing new regulatory definitions that could impact effectively every area of the American economy under a broad definition of data privacy, the FTC should carefully consider whether such an action is consistent with its current authority. I suggest that the FTC should also consider actions in light of its legal administrative discretion and in light of democratic values and the traditional separation of powers.

The approach to harm in the data privacy context should also utilize and build upon existing common law standards of harm. While there are concerns about the effects of certain elements of the tort system on innovation,[22] in general common law is able to provide an adaptable alternative to a static regulatory framework.[23] Rather than develop new regulatory requirements, regulators and regulated individuals and businesses may be able to adapt existing privacy torts to the concerns of harm in the digital age; or they may at least be able to provide a strong starting point for contextualizing when data privacy harm—and when, if ever, nonmarket harm—may be significant enough to require redress. Still, in general, such decisions should be addressed through adjudication in the courts as a reflection of emerging common law norms rather than as edicts from an administrative agency.[24]

The FTC's current approach has recognized many of these benefits of common law and in its own way it has built a common law of consent decrees with regard to data privacy.[25] Yet, while consent decrees have the advantages of flexibility and adaptability of common law, they lack the certainty and guidance for innovators that true common law provides.[26] Even in the current system

---

[19] *See* Andrea O'Sullivan, *How to Promote Data Privacy While Protecting Innovation*, THE BRIDGE, Feb. 13, 2019, https://www.mercatus.org/bridge/commentary/how-promote-data-privacy-while-protecting-innovation.

[20] *See* Brent Skorup & Jennifer Huddleston Skees, *It's Not About Facebook, It's About the Next Facebook*, REAL CLEAR POLICY, June 1, 2018, https://www.realclearpolicy.com/articles/2018/06/01/its_not_about_facebook_its_about_the_next_facebook_110654.html.

[21] *See* Jennifer Huddleston & Andrea O'Sullivan, *New GAO Report Says It's Time for Federal Data Privacy Legislation. But What Kind?*, THE BRIDGE, Feb. 25, 2019, https://www.mercatus.org/bridge/commentary/new-gao-report-says-its-time-federal-data-privacy-legislation-what-kind.

[22] *See* Jennifer Huddleston Skees & Trace Mitchell, *New Scooter Lawsuits Threaten Innovation*, ORANGE COUNTY REGISTER, Nov. 16, 2018, https://www.ocregister.com/2018/11/12/new-scooter-lawsuits-threaten-our-innovation/; Adam Thierer, *When the Trial Lawyers Come for the Robot Cars*, SLATE, June 10, 2016, https://slate.com/technology/2016/06/if-a-driverless-car-crashes-who-is-liable.html.

[23] KOOPMAN ET AL., *supra* note 16.

[24] *See* Jennifer Huddleston, *Unprecedented: The Issue of Agency Action by Consent Order on Innovation*, PLAIN TEXT, Sept. 22, 2017, https://readplaintext.com/unprecedented-the-issue-of-agency-action-by-consent-order-on-innovation-b23ab7b09f42.

[25] *See id.*; *see also* KOOPMAN ET AL., *supra* note 16.

[26] Huddleston, *supra* note 24; KOOPMAN ET AL., *supra* note 16.

focused on economic harm, the lack of clear guidance or standards regarding data security or privacy can make it difficult for both regulated parties and the public to know what compliance looks like.[27] Expanding the definition of harm to include a variety of subjective injuries would only increase such uncertainty. If there is to be an expansion or change in the definition of harm, clear guidelines that are developed by statute or common law should be the basis rather than regulatory action.

The FTC should continue its approach to harm with a focus on clear measurable harms to consumer welfare. It should be cautious about embracing a broader definition of harm that could lead to negative consequences for innovation and consumer choice.

TRADEOFFS BETWEEN EX ANTE AND EX POST REGULATORY APPROACHES TO DATA PRIVACY

The definition of harm is not the only context in which changes to data privacy regulation are likely to result in unintended consequences. The FTC has generally taken an ex post approach to regulating data privacy—that is, regulating after a technology has emerged and been adopted by users. Other regulators, such as those in Europe, have chosen to regulate ex ante the emergence and adoption of new technologies. In general, I would suggest that the FTC continue its ex post approach that promotes innovation while providing redress when consumer harm occurs.

An ex ante approach addresses problems with data uses and data collection practices, whether or not actual harm to consumers has actually occurred. This approach to regulation generally targets means rather than ends, which is why it is likely to restrict beneficial uses of data for consumers.[28] Additionally, an ex ante approach could limit the development of new technological alternatives as developers become wary and risk averse in order to remain complaint with the law.[29]

The potential costly and restrictive impact of ex ante regulation can be seen in states that have passed laws regulating biometric information usage by private entities, notably among them Illinois.[30] Certain common features to social media platforms, such as photo tagging or photo-based games, have been unavailable to consumers and have become risky for companies to deploy as a result of the strict compliance requirements that regulate the collection and storage of such information in Illinois.[31] Perhaps more concerning is that an Illinois court has ruled recently that mere violation of such a law is sufficient for litigation to continue even if there is no evidence that harm to a consumer actually occurred.[32] Such regulations remain static as innovation continues to develop, thus depriving consumers of potential benefits of data usage even as a future version of the technology in question could serve the purposes of that regulation.

In contrast, the ex post approach, traditionally taken by the FTC, allows greater evolution in data usage and data privacy practices while still providing redress when consumers actually experience harm.[33] Not only does such an approach allow a broader range of options to encourage innovation to improve options for data privacy, it also provides potential redress in situations

---

[27] Huddleston, *supra* note 24; KOOPMAN ET AL., *supra* note 16.
[28] NEIL CHILSON, REGULATORY TRANSPARENCY PROJECT, WHEN CONSIDERING FEDERAL PRIVACY LEGISLATION (2018).
[29] *See id.*; *see also* ADAM THIERER, PERMISSIONLESS INNOVATION (2016).
[30] *See* Niya T. McCray, *The Evolution of US Biometric Privacy Law*, FOR THE DEFENSE, May 2018.
[31] *See* Ally Mariotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why.*, CHICAGO TRIBUNE, Jan. 17, 2018, https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.
[32] STUART D. LEVI ET AL., SKADDEN, ILLINOIS SUPREME COURT HOLDS THAT BIOMETRIC PRIVACY LAW DOES NOT REQUIRE ACTUAL HARM FOR PRIVATE SUITS (2019).
[33] KOOPMAN ET AL., *supra* note 16.

where data might have been wrongly used to a consumer's detriment or deceptively gathered that might not be anticipated or addressed by ex ante regulations.[34] By continuing to focus on those cases in which consumers are injured rather than on ex ante restrictions on certain practices, the FTC is more likely to successfully balance consumer protection and innovation.[35]

Still, there are tradeoffs to the ex post approach. First, it is focused on redressing what in some cases may have been preventable harm. (Yet in spite of good intentions, focusing only on what might go wrong can result in a precautionary mindset that would excessively constrain future technological developments.[36]) Second, even though ex post regulation is the more permissive approach, a case-by-case approach may signal regulatory uncertainty to developers as court settlements may prevent practices later deemed appropriate.[37]

To improve certainty does not require detailed regulation dictating a list of approved or forbidden practices, but in continuing an ex post approach, the FTC should consider clarifying what constitutes sufficient injury for the FTC to accept a claim of unfair or deceptive practice under its existing authority.[38] This does not necessarily require a stringent rulemaking. The FTC could clarify the legal triggers of enforcement action through various soft-law mechanisms that can be easily adapted to rapidly improving technology.[39]

Still, while recognizing the potential tradeoffs that exist, the ex post approach to data regulation seems to strike a better balance between the interests of innovators and consumers.

PRIVACY AND SPEECH: THE POTENTIAL FRICTION BETWEEN FIRST AMENDMENT RIGHTS AND DATA PRIVACY REGULATION

In the United States, freedom of speech has withstood legislative and court challenges with notably few exceptions. This precedent provides an additional consideration in designing data privacy regulation compared to other countries without such a robust free-speech tradition.

The internet has provided numerous platforms to engage in speech and lowered the barriers for reaching wide audiences.[40] Typically a right to privacy will require favoring one person's preferred right over the right to speech of another person or entity.[41] When the government decides through regulation of data privacy which speech about another person or entity will be prohibited, it must be extremely cautious to narrowly tailor such regulation so as to avoid unnecessarily prohibiting or burdening lawful speech in the process.[42] While there may be some cases where the correct balance will favor a right to privacy over speech, such limitations should look to existing limited regulation of speech-induced harm outside of the digital space rather than building an expansive definition that could place significant burdens on a medium that has generally expanded the availability of speech.

---

[34] *See* Chilson, *supra* note 28.
[35] *See Hearing before the Subcommittee on Economic and Consumer Policy of the House Committee on Oversight and Reform*, 116th Cong. (2019) (statement of Jennifer Huddleston).
[36] *See* Adam Thierer, *The Precautionary Principle in Information Technology Debates*, TECH LIBERATION FRONT, Apr. 4, 2011, https://techliberation.com/2011/04/04/the-precautionary-principle-in-information-technology-debates/.
[37] *See* Huddleston, *supra* note 24.
[38] *See* Chilson, *supra* note 28.
[39] See Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems*, 17 COLO. TECH. L.J. 37 (2019).
[40] *See* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 Yale L.J. 1805 (1995).
[41] *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, STAN. L. REV. 52 (2000): 1088–89.
[42] *See id.*

This strong tradition of free speech in the United States should give pause to those who would copy other countries' data privacy regulations. For example, while the GDPR requires countries to provide exemptions to protect free expression, it leaves such protection to interpretations that vary wildly between countries and courts and more generally strongly favors the deletion of content as a result of a request rather than seeking to balance between competing rights.[43] Notably, a right to be forgotten as currently provided by European law would raise serious First Amendment concerns in the United States for original content creators, such as journalists,[44] and the online platforms that would be responsible for removing information flagged for deletion.[45]

Because of America's long history and strong tradition of free speech, the potential of data privacy rights to curtail otherwise lawful speech must be carefully considered when contemplating data privacy regulations either through legislation or FTC actions. Failure to do so could result in serious constitutional concerns for such regulations or fundamental changes in America's values.

CONSIDERATION OF EXPANDED FTC DATA PRIVACY REGULATION OR PENALTIES OUTSIDE COMPREHENSIVE FEDERAL DATA PRIVACY LEGISLATION

Until Congress enacts comprehensive federal data privacy law—including federal preemption of states laws and clear administrative delegation—regulation or enforcement will likely fall to agencies like the FTC.[46] The FTC should therefore continue an approach focused on redress of injuries while seeking to provide clarity for innovators to remain compliant with existing data privacy law. In this regard, the FTC should also consider how flexible clarifications and collaborations through soft-law mechanisms such as working groups, best-practices comments, and frequently asked questions could provide clarity while still enabling a wide variety of innovation and consumer choices.[47]

Clear guidelines are important for providing innovators with regulatory certainty, especially if penalties or enforcement will ensue from noncompliance. Still, one concern in the current "common law of consent decrees" approach is the lack of certainty for innovators regarding what is considered an unfair or deceptive practice in data privacy until enforcement occurs.[48] Particularly if penalties are sought for more sensitive data or other specific carve-outs, the FTC should provide clear guidance for innovators on what will constitute consumer harm and also consider the potential limitations on regulatory knowledge of how data usage and privacy and security products might evolve.

The FTC should not consider itself toothless when it comes to data privacy and security. The FTC has been an active enforcer in providing redress for consumer harm while still allowing innovation to provide a variety of options for consumer preferences.[49] The FTC should carefully

---

[43] Daphne Keller, *Free Expression Gaps in the General Data Protection Regulation*, Center for Internet and Society, Nov. 30, 2015, http://cyberlaw.stanford.edu/blog/2015/11/free-expression-gaps-general-data-protection-regulation.
[44] *See* MICHAEL J. OGHIA, CENTER FOR INTERNATIONAL MEDIA ASSISTANCE, INFORMATION NOT FOUND: THE "RIGHT TO BE FORGOTTEN" AS AN EMERGING THREAT TO MEDIA FREEDOM IN THE DIGITAL AGE (2018).
[45] *See* Eric Goldman, *Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)*, Knight First Amendment Institute, https://knightcolumbia.org/content/course-first-amendment-protects-google-and-facebook-and-its-not-close-question.
[46] *See* HAGEMANN ET AL., *supra* note 39.
[47] *See id.*
[48] KOOPMAN ET AL., *supra* note 16.
[49] *See* FEDERAL TRADE COMMISSION, PRIVACY & DATA SECURITY: UPDATE: 2018 (2018).

consider whether or not its existing tools, including providing formal rules, penalizing bad actors, and providing redress for consumers, could be better utilized to address the concerns. While the additional regulatory rulemaking requirements in the Magnuson-Moss Warranty Act of 1975 face much criticism, they do not fully prevent the FTC from making formal rules.[50] While this rulemaking process is certainly cumbersome and time consuming, it still allows a path for regulatory action.

Whether addressing specific types of data or continuing a more general approach, the FTC should consider clarifying its view on harm to consumer welfare in this context. Additionally, it should look not only at the potential of expanded tools but also at how existing tools might be better utilized to properly address concerns around data privacy.

CONCLUSION

The FTC has spent the past 20 years regulating data privacy largely on a case-by-case basis. This approach has been part of the permissive regulatory framework that has allowed US firms to be innovative leaders in the information technology industry. As the FTC considers how to address concerns around data privacy, it should seek to retain the benefits of its current approach while providing greater clarity to consumers and regulated parties. In general, the approach should seek to maximize and encourage the benefits of innovation, including the use of data, while providing appropriate redress for those harmed and levying penalties for actors who infringe or evade the law.

[50] Kent Barnett, *Looking More Closely at the Platypus of Formal Rulemaking*, THE REGULATORY REV., May 11, 2017, https://www.theregreview.org/2017/05/11/barnett-platypus-formal-rulemaking/.