

December 21, 2018

Elisa Jillson, James Trilling, and Jah-Juin “Jared” Ho
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments of Neil Chilson -- Hearings on Competition and Consumer Protection in the 21st Century: Consumer Privacy, Docket ID: FTC-2018-0098

Dear Ms. Jillson, Mr. Trilling, and Mr. Ho:

Thank you for the opportunity to comment on the Federal Trade Commission’s upcoming hearing on consumer privacy. The FTC serves a critical role in advancing consumer welfare. A key part of that role is protecting consumer privacy, and I know from my time at the Commission that FTC staff are dedicated to understanding the difficult questions around this issue.

I write in my personal capacity to share my thoughts on selected questions asked by the FTC.¹ I do so in the context of a recent article I wrote as a member of a working group on cyber security and privacy in the Federalist Society’s Regulatory Transparency Project.² I have attached that article and reference it in my answers to the questions below.

RESPONSES TO SELECTED QUESTIONS

- **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?**

Rather than ask what categories of data are sensitive, the FTC should ask what categories of data present a heightened risk of substantial injury to consumers. Legal constraints and good policy require the FTC to focus its efforts on addressing substantial consumer injury. As a result, the FTC has historically described as sensitive the types of information that create a heightened risk of substantial injury to consumers.³ This is appropriate because data that presents a heightened

¹ See Federal Trade Commission, FTC Hearing on Competition and Consumer Protection in the 21st Century - February 2019, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019>.

² Neil Chilson, “When Considering Federal Privacy Legislation”, released by the Regulatory Transparency Project of the Federalist Society, December 4, 2018 (<https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Privacy-Legislation.pdf>).

³ See FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS at 59 (Mar. 26, 2012) (describing as sensitive “information about children, financial and health information, Social Security numbers, and precise geolocation data.”), <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers>. Risk is a function of the probability of an injury multiplied by the magnitude of that injury. See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1.1 at App. B p.46 (Apr. 16, 2018) (defining risk as “[a] measure of the extent to which an entity is

risk of substantial injury to consumers warrant greater protection and data that poses a lower risk of substantial injury warrant lesser protection.⁴ Consumers also expect stronger protections for the types of data that present a heightened risk to them.⁵ For these reasons, the FTC should focus on assessing risk to consumers from different categories of information, rather than on assessing an abstract measure of sensitivity.

- **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?**

The constraints that companies implement around their use of data – “privacy protections” in the nomenclature above – do and should be allowed to vary across various marketplace offerings for the same reason that we do not adopt blanket price or quality requirements for products and services. Consumer care about a wide range of product or service characteristics. They care about privacy protections, yes, but also price, convenience, efficacy, flexibility, reliability, and openness, and more. And consumers rank these preferences differently. Thus, imposing one-size-fits-all constraints would eliminate combinations of privacy protections, price, convenience, etc, that many consumers might prefer. Such an approach could increase constraints on data – privacy – but ultimately reduce overall consumer welfare.

The best way to implement such flexibility is by focusing on the outcomes of end uses of information. Uses that always cause substantial injury to consumers should be abandoned. Uses that raise significant risk of substantial injury to consumers should be undertaken with care and with the well-informed consent of the consumer. Uses where the benefits vastly outweigh the risks should be encouraged, while providing options to consumers who have different preferences.

In many cases, companies face strong market incentives to use data to benefit consumers. But where such incentives are lacking, government intervention might be appropriate.

threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.”), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

⁴ Providing heightened protection to *all* data about consumers would ignore the costs that such protections impose on consumers. Commissioner Maureen Ohlhausen said it well: “Some might argue that ... consumers benefit from any restrictions on companies’ use of consumer data. If consumers cared only about privacy, this might be true. But consumers also care about other values, such as convenience, price, efficacy, safety, flexibility, and reliability, and they constantly balance all these values.” Maureen K. Ohlhausen, “Why is the FCC insensitive to data sensitivity?,” *The Hill*, Sept. 22, 2016, <https://thehill.com/blogs/congress-blog/technology/297194-why-is-the-fcc-insensitive-to-data-sensitivity>. Imposing heightened restrictions on all data would eliminate consumer choices on how to balance these values.

⁵ Maureen K. Ohlhausen, “Why is the FCC insensitive to data sensitivity?,” *The Hill*, Sept. 22, 2016, <https://thehill.com/blogs/congress-blog/technology/297194-why-is-the-fcc-insensitive-to-data-sensitivity>.

- **Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers’ finances in a directly measurable way. Alternatively, a “non-market” injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission’s privacy enforcement and policy work be limited to market-based harms? Why or why not?**

The FTC’s privacy enforcement and policy work should focus on addressing tangible, objective injury for four reasons. First, the law often requires it. For example, Section 5 unfairness specifically requires that the FTC identify a substantial injury and balance that against benefits to consumers or competition.⁶ If certain injuries cannot be measured and balanced against benefits, they may not meet this legal requirement.

Second, and related, the FTC can best use its limited resources by focusing on tangible, objective injuries. Consumers will be worse off if the FTC neglects cases with tangible, objective injuries in order to pursue cases with intangible and subjective injuries. Most FTC privacy cases involve company practices that result in both consumer benefit and consumer injury. If the FTC stops objectively beneficial practices because of intangible, subjective injuries to some consumers, this imposes the subjective preferences of some consumers on others – depriving the latter of an objective benefit. The net result of such enforcement would objective harm to some consumers in order to provide an unquantifiable benefit to others. By focusing on tangible, objective injury the FTC can avoid this undesirable result.

Third, the FTC should focus on tangible, objective injuries because such injuries are more easily redressed, and thus FTC enforcement can do the most good to help consumers recover from such injuries. Harms that are difficult to measure are also difficult to redress in a just manner, resulting in remedies that are insufficient or overly compensatory.

Finally, the FTC should focus on objective, tangible harms because markets can better address subjective harms. Another way to describe a subjective harm is a failure to satisfy a consumer’s preference. Markets respond to all kinds of unmeasurable and variable consumer preferences by providing, for example, better tasting coffee, softer laundry detergent, or safer cars. Such preferences are difficult to measure and vary from one person to the next, yet companies respond by constantly iterating their products and services to see which match consumer preferences best. This process does not perfectly satisfy all consumer preferences; in a world with resource constraints, that is not possible. But because markets allow a multiplicity of solutions to emerge over time, they provide solutions that fit a wider range of consumer preferences.

⁶ 15 U.S.C. 45(n). *See also*, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (December 17, 1980), Reprinted in *International Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) (“Unfairness Policy Statement”).

- **In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?**

and

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

Government intervention to protect consumers is best justified when one has conclusive evidence that an injury has or is likely to occur. The form and timing of the intervention depends on the characteristics of the harm. Thus, if the practice presents tangible, immediate, irreversible, and catastrophic harm to others, prescriptive ex ante government regulation is justified. In many other cases, the proper form and time for intervention is a case-by-case enforcement action after an injury occurs. This is especially true if the practice offers demonstrated benefits but raises concerns about vague, minor, or intangible harms.

Some argue that ex post enforcement can punish but cannot prevent injury. While that is true about the specific practice addressed in any single enforcement action, it is also true that each enforcement action has a deterrent effect on the future behavior of others. One need only observe the client alerts that law firms send out after every significant FTC enforcement action.⁷ An ex post, case-by-case approach can prevent future harm by demonstrating the types of practices that violate the law.

In the attached paper, pages 9-10, I elaborate on the reasons to prefer case-by-case frameworks for privacy, including the benefits to innovation.

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

I briefly describe the existing frameworks and their various benefits and drawbacks in the attached paper, Section IV, pages 6-9.

⁷ See, e.g., Megan L. Brown and Madeleine M. Lottenbach, “Your TV May Be Watching You, Too,” https://www.wileyrein.com/newsroom-newsletters-item-PIF_February_2017-Your_TV_May_Be_Watching_You_Too.html.

- **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?**

I describe key criteria for federal privacy legislation in Section V, pages 6-9, of the attached. In short, any federal privacy legislation should:

- preserve permissionless innovation to the maximum extent possible;
- avoid approaches or language that reinforce the idea that consumers *own* all data about them;
- maintain a clear distinction between privacy and data security;
- focus on regulating uses that injure consumers, rather than on restricting collection;
- clarify the application of the FTC's unfairness and deception authority, rather than mandate best practices;
- not give the FTC broad rulemaking authority.

CONCLUSION

Thank you for considering my comments as you develop the agenda and topics for the upcoming hearing. If I can be of any further assistance, please contact me at

Neil Chilson

Member, Cyber and Privacy Working Group,
Federalist Society's Regulatory Transparency Project

Senior Research Fellow, Technology and Innovation
The Charles Koch Institute & The Seminar Network Institute