

**Before the
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580**

December 21, 2018

In the Matter of)
)
21st Century Hearings Consumer Privacy) FTC Docket No.2018-0098-0003
and Questions for Comment)
)

**Submitted by
Wayne T. Brough**

**On Behalf of the
Innovation Defense Foundation**

The Innovation Defense Foundation (IDF) is pleased to submit these comments on the privacy aspects of the Federal Trade Commission’s (FTC’s) “Hearings on Competition and Consumer Protection.” The IDF is a nonprofit, nonpartisan, research and issue-advocacy institution focusing on “permissionless innovation,” seeking to address unnecessary legal or regulatory impediments to innovation. The Foundation is actively involved in several issues relating to the evolution of the internet and the digital economy. Consumer privacy is a critical component of this ecosystem, and the Innovation Defense Foundation commends the FTC for addressing this important yet complex issue. The IDF comments address privacy concerns more generally, but where appropriate the comments are linked to questions raised by the FTC.

- **General Question (first bullet point): What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and**

use? To what extent do consumers today, or are consumers likely to, realize these benefits?

In the digital world, there are a wide range of issues affecting consumer privacy, from encryption policy to questions about the handling of sensitive consumer data. Privacy is critical for both consumers and businesses.¹ Ensuring the financial transactions and other transactions involving sensitive information can be conducted securely is vital for all parties involved. Without secure online data, the underlying trust for online transactions does not exist, threatening the potential for innovation and entrepreneurship in the online economy.

At the same time, for businesses to compete effectively online, they must be able to demonstrate an ability to protect their consumer data. This is why issues of encryption are of such importance, and, at the same time, controversial, given questions of national security and law enforcement. Finding the appropriate balance between these competing policy ends is challenging, as demonstrated by the debates surrounding the decryption of an iPhone in the case in San Bernardino, California.² A long-term solution to such challenges has yet to be reached, and the question of protecting the consumers data from government surveillance continues to be an issue. In this respect, updating the Electronic Communications Privacy Act (ECPA) is an important step towards updating privacy laws created before the evolution of today's internet ecosystem.

This issue is also important with respect to U.S. businesses competing in a global internet market. Providing backdoors to online communications, or even the threat of such backdoors,

¹ Alessandro Aquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," The Economics of Privacy (March 8, 2016). Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411. Available at

SSRN: <https://ssrn.com/abstract=2580411> or <http://dx.doi.org/10.2139/ssrn.2580411>

² "Apple rejects court order to help FBI unlock San Bernardino shooter's iPhone," ABC News, available at: <https://www.abc.net.au/news/2016-02-17/apple-ordered-to-aid-in-unlocking-california-shooters-phone/7177842>

can put American firms at a disadvantage relative to foreign companies that can guarantee no backdoors will be built to access private data. Resolving such concerns remains an important element of federal policy, but this is only one component affecting consumer privacy.³

- **General Questions (second bullet point): What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?**

Consumer data is at risk from other sources as well. This includes threats of data breach—both from government agencies and businesses—that compile large databases of sensitive consumer information. In addition, there are concerns over efforts to monetize consumer information by large platforms and other companies with access to personal information.⁴ Data protection standards and questions over ownership of consumer data are currently being debated as ways to address such concerns.

Another area of concern is the question of data breaches. Whether from government databases or private databases, a breach of sensitive consumer information can impose significant costs on large groups of people. Given the potential level of damage, establishing clear policies for addressing any data breach should be considered as part of any efforts to reform federal privacy policies. In the case of a data breach, the party involved should be required to alert consumers of the problem and work with the proper authorities to minimize the potential damage. Making any breaches public as quickly as possible can alert others of malicious activity, allowing opportunities to improve security and minimize the possibility of further

³ Patrick Eddington, “Secrecy, Privacy, and the Future of American Liberty,” available at: <https://www.cato.org/publications/commentary/secrecy-privacy-future-american-liberty>

⁴ Ginger Zhe Jin, “[Artificial Intelligence and Consumer Privacy](#),” in [The Economics of Artificial Intelligence: An Agenda](#), Agrawal, Gans, and Goldfarb, forthcoming, 2018

breaches. Consumers should also be informed so they can take the necessary steps to limit the damage of any breach.

- **General Questions (thirteenth bullet point): To what extent do companies compete on privacy? How do they compete? To what extent are these competitive dynamics dictated or influenced by consumer preferences, regulatory requirements, or other factors?**

It must be remembered that there is a demand for privacy as a good in the marketplace. Both consumers and businesses have a demand for privacy, and markets should be allowed to evolve in order to satisfy that demand. This means avoiding mandates that eliminate the flexibility of those trying to develop products that enhance privacy. The market for privacy should remain flexible in order to promote innovation and entrepreneurship with respect to privacy.

To be successful, businesses must compete and provide better services for consumers, and better information is one source of competition. It allows more customized marketing in products, reduces fraud, and lowers costs. At the same time, consumers in the private sector can exercise choice. Consumers value privacy and businesses are realizing this, and they are beginning to compete based on privacy policies. Privacy policies in the future must consider the benefits of these information-sharing practices.

- **Questions About Legal Frameworks: (first bullet) What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each?**

The FTC's inquiry into consumer privacy is timely and important; the agency's work can help develop transparent and open standards for resolving such questions. And establishing a

risk-based approach can provide the flexibility to address these questions in an efficient manner. When undertaking such analyses, the Innovation Defense Foundation encourages the FTC to also include a thorough benefit-cost analysis in order to ensure any federal regulations or other mandates in this area generate benefits in excess of the costs of complying with any new standards.

This is important, given the evolution of privacy regulation in the United States. Historically, the Constitution was vague with respect to privacy, making it difficult to define specific rights to privacy.⁵ As a result, the federal courts have developed privacy law based on various amendments to the Constitution. In addition, broader laws were developed pertaining to specific sectors of the economy, such as health care, finance, and education, where sensitive information is collected on individuals. These sectoral laws dominate privacy policy in the United States, and where additional privacy policy issues arise, the FTC has the authority to intervene.

This stands in stark contrast to other approaches to privacy, such as that adopted by the member nations of the European Union, where privacy rights are more clearly defined, and broad mandates have been developed to protect consumer privacy.⁶ While more direct, the EU's approach to privacy raises significant questions with respect to administrative costs and the economic burden of compliance.

For example, the GDPR, or General Data Protection Rule, approved by the EU in 2016 and implemented in 2018, includes sweeping new mandates affecting all companies operating

⁵ Downes, Larry, A Rational Response to the Privacy 'Crisis' (January 7, 2013). The Cato Institute, Policy Analysis #716, January 7, 2013. Available at SSRN: <https://ssrn.com/abstract=2200208> or <http://dx.doi.org/10.2139/ssrn.2200208>.

⁶ Avi Goldfarb & Catherine Tucker, 2012. "[Privacy and Innovation](#)," *Innovation Policy and the Economy*, University of Chicago Press, vol. 12(1), pages 65 - 90.

online doing business with EU citizens.⁷ The law imposes new standards for data protection as well as requirements for large firms to assign Data Protection Officers to ensure compliance with the regulations. While the laws are still being put in place, it is clear that the administrative costs will be significant, perhaps to the detriment of both consumers and innovation.

One particular issue of note is the limited scalability of the EU's data protection standards. Given the substantial burdens of compliance, large incumbent tech companies are better suited to comply with the administrative costs. Smaller players and startups in the market may find the costs prohibitive, forcing them to leave the market or narrow their functions. Scalability should be a critical component of the administration's privacy policies. Efforts should be made to establish flexible standards with a risk-based approach to compliance. In other words, the standards should be commensurate to the risk associated with data being collected. At the same time, privacy policy should provide flexibility for small and medium sized businesses, where the administrative burden can thwart new entrants in the marketplace.

Accordingly, both the Regulatory Flexibility Act and the Small Business Regulatory Enforcement Fairness Act review process must be important components of any rulemaking process addressing privacy concerns. Reviews under Paperwork Reduction Act should also be considered carefully to ensure no disproportionate burdens are imposed on small and mid-sized businesses. Such analyses will further the FTC's goals of providing risk-based flexibility while creating a more comprehensive framework for privacy policy. The overall goal of privacy regulations should focus on outcomes and performance-based standards that provide those affected by federal policies a large degree of flexibility with respect to how they comply.

⁷ See "GDPR Key Changes," EU GPDR.org, available at: <https://eugdpr.org/the-regulation/>

- **Questions About Legal Frameworks (second bullet): What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?**

Evaluating privacy laws from an institutional perspective is important; the correct framework will reduce the transactions costs of addressing challenges with respect to privacy law. In this regard, ex post, risk-based enforcement may provide greater flexibility in addressing privacy concerns. Ex ante regulatory solutions by nature are more prescriptive and may prove difficult to apply in all situations. Addressing many concerns ex post allows risk-based enforcement that can be adjusted commensurate to the cost of the privacy incursion.

One area where ex ante regulations may prove more suitable is when establishing baseline policies, such as how to address a data breach. In such instances, providing both firms and consumers a clear understanding of what process must be followed may prove useful, especially given the information asymmetries between the two groups.

- **Questions About Legal Frameworks (third bullet): The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct? Why or why not?**

In this regard, the current sectoral approach to privacy in the United States, in conjunction with FTC authority to address any additional privacy concerns, provides a

framework for privacy policy that avoids the excessive burdens generated by the EU's approach to privacy regulation. While there may be opportunities for improvement and establishing a common baseline for privacy policy, any changes must be assessed from a benefit-cost perspective. In some ways, the sectoral approach has granted a degree of flexibility with respect to how privacy policy has developed in various parts of the economy, and those specialized policies must be evaluated against any broader federal baselines that are proposed.

Ideally, any new federal policies will be technologically neutral so as not to bias market outcomes. And to the extent possible, federal policy should strive to be sector-neutral as well, with little or no distinction between privacy mandates for online and offline data use. Consumer data may be at risk in both instances, and federal privacy policy should ensure that consumers enjoy the same protection of their data in any situation.

- **Questions About Legal Frameworks (sixth bullet): 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?**

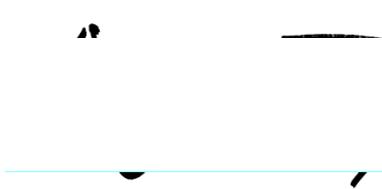
The question of harmonization must be addressed both with respect to federal-state policy differences, as well as differences across countries. Given the borderless nature of the internet, state level regulations and regulations emanating from other countries affect U.S. internet policies. When considering state-level privacy policies, federal pre-emption is an option that must be evaluated carefully. Complying with different state privacy mandates can hamper innovation and limit economic activity. At the same time, evaluating the various state policies with respect to privacy may assist in identifying best practices in the case of federal preemption. The Innovation Defense Foundation encourages the FTC to conduct such an analysis of state

privacy laws, identifying the appropriate role for federal preemption. The goal for such an exercise is to identify those policies that address privacy concerns while facilitating innovation.

Conversely, federal policy must also address concerns raised by other nations with respect to privacy. The United States and the EU have established the Privacy Shield and the United States must demonstrate that its privacy practices provide sufficient protections for protecting data under this framework.⁸ Identifying the appropriate federal privacy baselines assist in our international negotiations on privacy.

In conclusion, the International Defense Foundation appreciates the FTC's efforts to clarify federal privacy policies. The FTC has raised important questions for assessing federal privacy policy, including harmonization, and risk-based outcomes that develop policies proportionate to the potential threat of exposure. Privacy is an important issue that is becoming more prominent as more activity moves online. To the extent that the FTC can utilize benefit-cost analysis in its assessment of federal policy it will improve final outcomes by striving to ensure policy outcomes where benefits of federal privacy policy exceed the costs.

Respectfully submitted,


Wayne T. Brough, PhD
President
Innovation Defense Foundation
600 F Street, NW Floor 5
Washington, DC 20004

⁸ "Privacy Shield Framework," International Trade Administration, <https://www.privacyshield.gov/welcome>,

