Comments filed with the Federal Trade Commission Regarding Hearing on "Competition and Consumer Protection in the 21st Century"

December 2018

Thomas M. Lenard

409 12th Street SW ● Suite 700 ● Washington, DC 20024
Tel: (202) 828-4405 ● Email: info@techpolicyinstitute.org ● www.techpolicyinstitute.org

Hearings on Competition and Consumer Protection in the 21st Century

Pre-Hearing Comments of Thomas M. Lenard, Senior Fellow and President Emeritus

Technology Policy Institute

I am submitting these comments in connection with the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century. These comments respond to questions raised in the FTC's announcement.[1]

Summary of Major Points

My major points are as follows:

- Collecting and analyzing large amounts of data is the basis of much, if not most, of the innovation that has taken place on the internet over the past 20 years. Economists estimate that free content provided by advertising-supported platforms generates large benefits for consumers. While these platforms have suffered well-publicized data breaches, systematic evidence of privacy-related harms even from these episodes is difficult to find.
- Many of the benefits from data are realized when data are reused, combined with other data sets, and used to answer new questions that were not anticipated at the time the data were collected. The European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) restrict these practices.
- Markets appear to work. Consumers willingly exchange some personal information for the resulting benefits despite what they say in many surveys. Firms suffer large financial repercussions when they experience data breaches, creating an incentive to avoid them. These factors suggest that the markets for privacy and data security are not subject to serious market failure.
- Any new proposed privacy policy should yield net benefits relative to the current Federal Trade Commission (FTC) approach, which is the relevant baseline. The FTC approach is *ex post* enforcement based on actual harms. In contrast, the GDPR and CCPA use an *ex*

[1] https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019.

ante regulatory approach that limits the collection, use, sharing, and retention of data in an attempt to protect consumers from hypothetical harms.

- Privacy benefits are a reduction in privacy harms. Any new policy should focus on outcomes, rather than dictate specific practices. The relevant outcome should be a reduction in privacy harms to consumers.
- Theory and evidence suggest that privacy regulations favor large incumbents and make entry by new firms more difficult. Indeed, thus far companies like Google and Facebook appear to be benefiting from GDPR. Smaller companies are leaving the European market to avoid these costs and the risk of large fines for noncompliance.
- Preempting state privacy laws is likely to yield benefits because the affected markets are national in scope, but only if a national law is significantly better—i.e., places fewer restrictions on the use of information—than the CCPA.
- The FTC's current *ex post* enforcement approach based on actual harms has many advantages relative to the *ex ante* regulatory approach reflected in the GDPR and CCPA. Abandoning the current *ex post* approach would likely entail substantial costs to consumers and producers of digital goods and services.

The Value of Information

The Commission asks about the actual and potential benefits and risks for consumers and to competition of information collection, sharing, aggregation, and use.

The information technology revolution has enabled firms to collect, store, and analyze massive amounts of data at relatively low cost. This data revolution is behind much, if not most, of the innovation that has taken place on the internet over the past 20 years and is integral to current developments in artificial intelligence and machine learning.

"Attention platforms,"[2] such as Google and Facebook, are a principal target of privacy regulations, such as the GDPR and CCPA. These platforms have suffered well-publicized data breaches. Despite these breaches, however, systematic evidence of privacy-related harms is

[2] David Evans, "Attention Platforms, The Value of Content, and Public Policy," forthcoming, *Review of Industrial Organization*.

difficult to find.[3] Asserting that collecting information or sharing information with third parties is harmful *per se* does not make it true.

While evidence of harms is minimal, the benefits of these platforms are large. In the language of economists, they solve an important transaction cost problem by acting as an intermediary between consumers and marketers. Consumers benefit because of the content they receive—e.g., access to a search engine. Production of this content is possible because the marketers are able to collect data and deliver advertising messages to consumers when they are spending time on (i.e., devoting attention to) the platform. Better data produce better targeted advertising, which yields better information to consumers and increases the revenues available to platforms to invest in content that is often provided to consumers free of charge. Economists estimate that free content on the internet generates large benefits for consumers.[4]

Customer data are also used to develop new products and services that consumers value. Netflix, for example, uses viewing data to inform its development of original content.[5] Data can also be used to improve algorithms and protect against security threats, and notify buyers of a product of important recalls.

As the use of large data sets for artificial intelligence, machine learning, and other purposes has become more common, the value of online data is increasing. The Obama Administration's President's Council of Advisors on Science and Technology (PCAST) noted in a report on big data that "[t]he beneficial uses of near-ubiquitous data collection are large, and they fuel an increasingly important set of economic activities."[6] The World Economic Forum noted that data can be used to make financial services more inclusive, improve education, expand health coverage, and improve agricultural productivity.[7] The McKinsey Global Institute described additional potential benefits in health care, government services, fraud protection, retailing, and

[3] Thomas M. Lenard, Comments to FTC, Informational Injury Workshop P175413, Oct. 2017, https://techpolicyinstitute.org/wp-content/uploads/2017/10/TLenard_Informational-Injury-Workshop.pdf.
[4] *Id*. Also, see also Eric Bryinjolfsson and Joo Hee Oh, The Attention Economy: Measuring the Value of Free Digital Services on the Internet, available at https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1045&context=icis2012
[5] See Michael D. Smith and Rahul Telang. 2016. Streaming, Sharing, Stealing: Big Data and the Future of Entertainment. MIT Press, Cambridge, MA.
[6] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective, May 2014, p. x, https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy.
[7] The World Economic Forum, "Big Data, Big Impact," 2012, http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf.

manufacturing.[8] A 2014 White House report on big data observed that "properly implemented, big data will become an historic driver of progress."[9]

Many of these benefits are realized when data can be reused, combined with other data sets, and used to answer new questions that were not anticipated at the time the data were collected. Innovations often come from using multiple sources of data, which may include transferring data to third parties. That approach can enhance the value of data for purposes ranging from epidemiology studies to marketing. Eliminating the "option value" of future use and serendipitous results makes data less valuable.

The Question of Market Failure

The Commission asks several questions relating to whether the market adequately reflects consumers' privacy preferences and whether firms have sufficient incentives to respond to those preferences. The experience of both consumers and businesses suggests that the markets for privacy and data security are not subject to serious market failure.

The market provides information on how consumers evaluate the tradeoffs involved in sharing information and how much they are willing to pay for more privacy. Economists usually base consumers' willingness-to-pay on observed market behavior, since how people behave when confronted with actual market choices better reflects their real preferences than responses to survey questionnaires or even behavior observed in experiments. The widespread use of free, advertising-supported services, such as search, email, and online news subscriptions, suggests that people routinely and voluntarily give up some information about themselves in return for access to content, more useful advertising, and other services, although the transaction is indirect. That is, consumers often are willing to exchange less privacy for the resulting benefits.

A recent paper by Athey, Catalani, and Tucker supports this observation.[10] Their work highlights the "privacy paradox: [w]hereas people say they care about privacy, they are willing to

[8] McKinsey Global Institute, "Big Data: The Next Frontier for Innovation, Competition, and Productivity," May 2011, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.
[9] Executive Office of the President, "Big Data, Seizing Opportunities, Preserving Values," May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[10] Susan Athey, Christian Catalini, and Catherine Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *NBER Working Paper Series*, Sept. 27, 2017, https://www.nber.org/papers/w23488.

relinquish private data quite easily when incentivized to do so."[11] Their results suggest, "[w]hen expressing a preference for privacy is essentially costless as it is in surveys, consumers are eager to express such a preference, but when faced with small costs this taste for privacy quickly dissipates."[12]

Businesses also evaluate the tradeoffs involved in collecting, using, and safeguarding the information they hold. Firms have a strong incentive to avoid data security breaches because markets penalize them if breaches occur. Costs include direct costs of addressing the breaches as well as potentially substantial reputational effects, as companies from Target to Equifax to Facebook quickly learn.

These costs are reflected in stock prices. Spanos and Angelis reviewed the literature on the impact of information security events on stock prices.[13] Of the 28 studies that analyzed the impact of security breaches on the breached firm, 25 (89 percent) found a negative impact.[14] In 20 of those studies (80 percent), the negative impact was statistically significant.[15] Equifax, for example, lost about $6 billion in market capitalization after its breach.[16] In a span of a week after the Cambridge Analytica episode became public, Facebook shareholders saw their equity value decline by 14 percent.[17]

The Relevant Baseline

The Commission asks about the "tradeoffs between *ex ante* regulatory and *ex post* enforcement approaches to privacy protection."

The FTC should analyze whether any new approach it considers is likely to yield net benefits relative to the *status quo*, which is the agency's current approach of *ex post* enforcement. Such a

---

[11] *Id*. at 2.
[12] *Id*. at 5. The authors offer a caveat to their finding: "On the one hand it might lead policy makers to question the value of stated preferences when determining privacy policy. On the other hand, it might suggest the need for more extensive privacy protections, from the standpoint that people need to be protected from their willingness to share data in exchange for relatively small monetary incentives." *Id*. at 18.
[13] George Spanos and Lefteris Angelis, "The Impact of Information Security Events to the Stock Market: A Systematic Literature Review," *Computers & Security*, 58 (2016), 2016-2029.
[14] *Id*.
[15] *Id*.
[16] https://www.cnbc.com/2017/09/14/equifax-will-not-survive-fallout-from-massive-breach-says-technology-attorney.html.
[17] Thomas Lenard, "Facebook-Cambridge Analytica: Is It Time to Regulate the Internet," https://techpolicyinstitute.org/press_release/facebook-cambridge-analytica-is-it-time-to-regulate-the-internet/.

demonstration involves showing that the new approach addresses actual harms the FTC cannot or does not address. Since benefits are a reduction in harms, if there are no harms, there can be no benefits, only costs. If there are benefits, the Commission still needs to demonstrate that those benefits are sufficient to outweigh the costs associated with having less information available.

The *ex ante* approach represented by the GDPR and CCPA contrasts with the current *ex post* approach practiced in the U.S. and enforced by the FTC. As recently explained by former Acting FTC Chairman Maureen Ohlhausen:

> Our primary privacy and data security tool is case-by-case enforcement under Section 5 of the FTC Act to protect consumers from deceptive or unfair acts or practices. One significant benefit of this approach is that it limits the need for policymakers to predict future developments in the marketplace. This is especially important in the complex, fast changing technology industry and in areas such as privacy, where consumers have a wide range of evolving expectations and preferences. Case-by-case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. Each case integrates feedback on earlier cases from consumers, industry, advocates, and, importantly, the courts. This ongoing process recognizes that markets, consumer expectations, and consumer benefits and risks evolve with new technologies, and it protects consumers while allowing innovation to occur.[18]

The FTC's *ex post* enforcement-based approach has many advantages over an *ex ante* regulatory approach that prophylactically limits the collection, use, sharing, and retention of data in an attempt to protect consumers from hypothetical concerns about data being used in harmful ways. The *ex post* approach is based on actual harms and therefore more likely to improve consumer welfare.

The NTIA's Request for Comments

The Commission's announcement refers to the National Telecommunications and Information Administration's (NTIA) recent Request for Comments (RFC) on the Administration's approach to consumer privacy.

[18] Maureen K. Ohlhausen, Remarks at the FTC Informational Injury Workshop, Dec. 12, 2017, https://www.ftc.gov/system/files/documents/public_statements/1289343/mko_speech_-_info_injury_workshop_1.pdf.

In its RFC, the NTIA stated that "[r]isk-based flexibility is…at the heart of the approach the Administration is requesting comment on."[19] Further, the NTIA proposed that "discussion of consumer privacy in the United States refocus on the outcomes of organizational practices, rather than on dictating what those practices should be."[20]

A risk-based approach that focuses on outcomes, rather than rules, could be a positive step toward developing policies that can pass a cost-benefit test and maximize net benefits to consumers. However, any such approach would need to clearly define the harms it proposes to address and explain why the proposed approach is better than the FTC's current approach.

Identifying harms is difficult. During the last administration, the government issued at least five reports that failed to present evidence that data used for commercial and other non-surveillance purposes caused actual privacy harms.[21] Discussions of harm in these reports was hypothetical and speculative.

Even in the area of data breaches, where one might expect better data because the costs might be more easily measurable, accurate data are unavailable. For example, the estimates of the total losses from the 2013 data breach of department store retailer Target Corporation range from $11 million to $4.9 billion.[22] It is difficult to find evidence of harms associated with well-publicized quasi-data breach episodes, such as Facebook-Cambridge Analytica.[23] The FTC, with its research capabilities, could make an important contribution by measuring harms associated with data security, and the effects of policies in reducing harms.

Focusing on outcomes could mean something analogous to a performance standard in other areas of regulation. For example, an environmental performance standard might specify a maximum

---

[19] 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018).
[20] *Id*. at 48601.
[21] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," May 2014; President's Council of Advisors on Science and Technology, "Report to the President, Big Data and Privacy: A Technological Perspective," May 2014 (PCAST Report); The White House, "Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 2012; Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Mar. 2012; and Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014.
[22] Josephine Wolff and William Lehr, "Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data," Aug. 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2943867.
[23] *See e.g.* https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html.

level of a pollutant a plant would be permitted to emit, leaving the plant to determine how to meet this requirement at minimum cost. Using outcomes as the relevant measure in the privacy context would mean focusing on some measure of privacy or privacy harms—for example, data breaches or identity fraud—as the relevant output. The NTIA does not attempt to define such a measure.

Instead, the NTIA defines outcomes to include transparency, control, and access. But these are all inputs, not outputs, and imply that the government would be dictating practices, which the NTIA says it does not want to do. Moreover, NTIA does not explain how these inputs would produce privacy benefits—i.e., reduce privacy harms. The FTC could devote some resources to advancing our understanding of this issue.

The NTIA acknowledges that its "outcomes" underpin "many of the principle-based approaches, including FIPPs [Fair Information Practice Principles]."[24] However, the FIPPs approach to privacy has increasingly been criticized as irrelevant or counterproductive in the world of big data.

For example, for "control," according to the NTIA, "[u]sers should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations."[25] This would seem to imply a "Notice and Choice" framework, which has come to be seen as increasingly meaningless in the age of big data when many of the most productive uses of data are unpredictable. As the 2014 PCAST report noted, "[a]s a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data. It is simply too complicated for the individual to make fine-grained choices for every new situation or app."[26]

The NTIA also highlights the related issue of "transparency" as an outcome: "[u]sers should be able to easily understand how an organization collects, stores, uses, and shares their personal information."[27] The notion that consumers should understand how their data are being collected, used, and shared seems appealing, but in the big data era where hundreds of data points and

[24] *Id*. at 48601.
[25] *Id*.
[26] PCAST Report, p. 38.
[27] 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

complex calculations are used to create some kind of score or index, it is likely to be impractical and not especially meaningful to consumers. This activity cannot be meaningfully conveyed through a simple notice, and consumers would not devote the hours required to understand such descriptions. It would likely be impossible for consumers without the necessary technical training to understand how firms use data, even without time constraints.

Moreover, consumers routinely exchange their information for a variety of benefits without reading and understanding privacy notices, suggesting that most consumers do not find it rational to spend the time and effort to do so. Former FTC officials Howard Beales and Timothy Muris observe that "the reality [is] that decisions about information sharing are not worth thinking about for the vast majority of consumers…"[28] The recent PCAST report also addresses this issue, observing, "[o]nly in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[29]

Competition Considerations

The Commission asks about "the effects, if any, on competition and innovation from privacy interventions."

The competitive implications of privacy regulations should be particularly important for the FTC, given its dual consumer protection and competition missions. Theory and evidence suggest that such regulations favor large incumbents and make entry by new firms more difficult. This is reflected in the early experience with GDPR, which imposes large compliance costs. Companies like Google and Facebook are seen as benefiting relative to smaller advertising competitors under the new regime.[30] The Financial Times reports that smaller U.S. companies are pulling out of the European Union (EU) in reaction to the costs of complying with GDPR and the potential liability risks of doing business there.[31]

---

[28] J. Howard Beales and Timothy J. Muris, "Choice or Consequences: Protecting Consumer Privacy in Commercial Information," *University of Chicago Law Review*, Vol. 75: Iss. 1, Article 6 (2008), *available at* https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/6/.

[29] PCAST Report, p. xi.

[30] https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.

[31] https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04. *See also*, "GDPR as Europe's Tariff by Other Means?" http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.

The transactions costs to consumers of providing consent under consent-based privacy regulation also favors large firms that offer a range of services. Small firms and new entrants are likely to be adversely affected because consumers incur larger transactions costs reading notices and indicating consent for a range of firms relative to, for example, a single firm offering the same set of services.[32]

Finally, making it more difficult for data to be sold or otherwise transferred to third parties is a barrier to entry. Firms entering a market often need data on characteristics and preferences of their potential customers before they can start to collect their own data from actual customers. If the data entrants can obtain from third parties becomes more costly and/or of lower quality due to restrictions on data sharing, it may be more difficult for them to succeed.

GDPR and CCPA— Harmonization, Interoperability, and Preemption

The Commission's notice refers to the fact that "some jurisdictions have enacted new laws that contain new approaches for addressing privacy risks." The Commission also asks the related question of whether new federal privacy legislation, if enacted, should be based on the FIPPs.

A major challenge for U.S. policy makers is how to respond to the European GDPR that became effective earlier this year[33] and the recently-enacted CCPA, scheduled to become effective at the beginning of 2020.[34] The GDPR applies to the data of EU citizens and the CCPA applies to businesses that operate in California.

While the GDPR and the CCPA differ in important ways, they both limit the collection, use, sharing, and retention of data.[35] The FIPPs dating back to the 1970s,[36] the Organization for

[32] Campbell, James David, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," *Journal of Economics & Management Strategy*, 24(1): 47-73 (Spring 2015), *available at* https://ssrn.com/abstract=2564799 or http://dx.doi.org/10.1111/jems.12079.
[33] https://eugdpr.org/ (Apr. 14, 2016, effective May 25, 2018).
[34] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (Jun. 28, 2018, effective Jan. 1, 2020) (California's Consumer Privacy Act of 2018).
[35] For example, the GDPR has more stringent consent requirements for the collection of consumer data, while the CCPA has more stringent consent requirements for sharing those data with third parties.
[36] An excellent summary of the evolution of the FIPPs comes from Robert Gellman, "FAIR INFORMATION PRACTICES: A Basic History", last updated Nov. 11, 2013, *available at* http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf, and the current FTC FIPPs are posted at http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Economic Cooperation and Development's (OECD's) Privacy Principles,[37] and the Obama Administration's Consumer Privacy Bill of Rights[38] all take a similar approach.

Any regulation that restricts the use of information represents a tradeoff between the benefits of increased privacy and the cost of decreased information in the marketplace. Those costs will likely show up in decreased availability of content for consumers, a decline in innovation, and lower economic growth.

An important question is how the GDPR and the CCPA (and perhaps other state regulations) affect the cost-benefit calculus. One might argue, for example, that the U.S. should adopt a national regime following GDPR and CCPA, even if such a regime would not otherwise pass a cost-benefit threshold.

Global companies with significant business in Europe and California will likely need to comply with both sets of requirements even though compliance will be expensive. Forbes estimated that U.S. Fortune 500 and U.K. FTSE 350 companies spent nearly $9 billion ahead of the May 25 GDPR effective date.[39] While large companies probably can't avoid these expenditures, smaller companies may be able to. As the Forbes article notes, "There are two ways of avoiding GDPR—stop doing business in Europe entirely, or dump the personal data you're holding—and both are proving popular."[40]

For a global company that is already complying with GDPR, the incremental costs of a similar regime in the U.S. would be small. Such companies might have an interest in seeing a GDPR-type of regime adopted in the U.S., because it would impose large costs that might not be avoidable for smaller competitors. For startups, the costs of such a regime would be a major barrier to entry.

The considerations with respect to CCPA are somewhat different, since a federal statute could preempt state laws. There is a strong rationale for preemption because the affected markets are national in scope. Without preemption, firms operating nationally would be forced to comply

[37] http://www.oecd.org/sti/ieconomy/privacy.htm.
[38] https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.
[39] https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#4613b15a34a2.
[40] *Id*.

with the most stringent state requirements and perhaps also have to deal with inconsistent state laws. It is likely better to have privacy policy set at the national level, by lawmakers who presumably represent the nation as a whole, rather than have one state or set of states effectively "preempt" the rest of the country.

A national policy that preempted the states would make sense on cost-benefit grounds if the federal regulations were significantly better than the CCPA—i.e., placed fewer restrictions on the use of information and had a better balance of benefits and costs.

Conclusion

The FTC's current *ex post* enforcement approach based on actual harms has great advantages relative to the *ex ante* regulatory approach reflected in the GDPR and CCPA. While there is a strong argument in favor of a national regime that would preempt state laws, there likely would be substantial costs associated with abandoning the current approach in favor of some variant of the approach taken by the GDPR and the CCPA—a GDPR- or CCPA-light.