

Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005

August 20, 2018

Donald Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex C)
Washington, DC 20580

RE: Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201

Dear Secretary Clark,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the request for comment (RFC) from the Federal Trade Commission (FTC) on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy.¹

ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

Please find our response to the following topic:

THE INTERSECTION BETWEEN PRIVACY, BIG DATA, AND COMPETITION

Data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market

¹ "Hearings on Competition and Consumer Protection in the 21st Century," Federal Trade Commission, n.d.
<https://www.ftc.gov/policy/hearings-competition-consumer-protection>.

With the increased power and decreased cost of collecting, transmitting, and storing data, as well as an increase in machine-readable data, more and more companies are using more and more data to help them provide goods and services. However, a number of commentators have begun to argue that, in the case of companies aggregating large amounts of data, competition policy should be extended to incorporate concerns about the collection and use of data beyond clear examples of anticompetitive behavior.² The general argument is that the mere act of collecting large amounts of data, such as the vast quantities of personal data collected by social-networking platforms, search engines, and e-commerce sites, gives companies an unfair competitive advantage and that competition policy needs to incorporate this analysis.³

To date, U.S. regulators have not adopted this line of reasoning, nor should they. While it is true that data can be used in anticompetitive ways, competition policy is capable of dealing with such abuses. In fact, when analyzing allegations of such behavior, it is often helpful to imagine whether agencies would object if the activity complained about involved some input of critical importance other than data. This helps clarify whether the threat to competition is truly due to control of an important resource or to ungrounded fears about the uniqueness of data.

² For the most comprehensive argument see Maurice E. Stucke and Allen P. Grunes, *Big Data and Competition Policy* (New York: Oxford University Press, 2016).

³ Margrethe Vestager, “Big Data and Competition” (speech before the EDPS-BEUC Conference on Big Data, Brussels, September 29, 2016), http://ec.europa.eu/commission/2014-2019/vestager/announcements/big-data-and-competition_en; European Commission, “Online Platforms and the Digital Single Market Opportunities and Challenges for Europe” (communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, May 25, 2016 COM(2016) 288), 13, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288>. See also UK Competition and Markets Authority (CMA), “Online Platforms and the EU Digital Single Market” (written evidence, (OPL0055), CMA, London, October 23, 2015), <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internalmarket-subcommittee/online-platforms-and-the-eu-digital-single-market/written/23391.html>. “To the extent that such data is of central importance to the offering but inaccessible to competitors, it may confer a form of ‘unmatchable advantage,’ making it hard for those competitors to compete”; Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy, “Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by ‘Big Data,’” (Paris: OECD, Directorate for Science, Technology and Industry, June 18, 2013), [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP\(2012\)9/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En). “Data are a core asset that can create significant competitive advantage and drive innovation, sustainable growth, and development.”

Advocates for intensifying competition policy cite a variety of purported flaws in the current system. However, ITIF, as well as other defenders of the current approach seldom argue that there can be no anticompetitive behaviors when it comes to data. Rather, ITIF and others say that, in some cases, data use—rather than data collection—could trigger competitive concerns.⁴ What defenders do argue is that, when it comes to competition policy, the focus should be on abusive behavior and not on structural issues, such as how much data a company holds. Extending competition review to examine the level of data companies hold will send a signal to companies that they should not do the hard work of collecting data, most of which is used to expand social and economic welfare.

The collection of large amounts of data does not by itself represent a threat to competition. Although use of data might in specific circumstances justify regulatory intervention, in most cases the acquisition and use of data does not reduce competition, and the existing legal framework, including traditional interpretations of existing statutes, gives competition and data protection regulators all the flexibility they need to protect markets and consumers. On the contrary, large amounts of data, including personal information, are increasingly a vital input for some of the economy's most important innovations, including online platforms, medical diagnoses, digital assistants, language translation, urban planning, and public safety. Moreover, data is non-rivalrous: Multiple companies can collect, share, and use the same data simultaneously. That goes for consumers, too: When consumers “pay with data” to access a website, they still have the same amount of data after the transaction as before, allowing them to share the same data with multiple companies.

Finally, it is important to note that some of the platforms that collect large amounts of consumer data are natural monopolies: they gain significant market share because of economies of scale and scope, and what economists call “network effects.” By providing platforms for users around the world to connect, their very size generates enormous economic benefits for society and consumers. These platforms serve two-sided markets, and many of these businesses, especially those provided free services, face competition on the advertising side.

Competition on privacy and data security attributes (between, for example, social media companies or app developers), and the importance of this competition to consumers and users;

Proponents of expanding the scope of antitrust review to incorporate how companies collect and use data make a variety of arguments. In a paper that largely rejects these claims when applied to concerns about

⁴ Daniel Castro, “Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help,” Center for Data Innovation, November 6, 2017, <http://www2.datainnovation.org/2017-open-apis.pdf>.

privacy, FTC Commissioner Maureen Ohlhausen and attorney Alexander Okuliar list four arguments proponents make:

1. Privacy is a non-price dimension of competition that can be hurt if some companies have too much market power.
2. Antitrust authorities should not focus solely on the impact on competition in cases where competitive agreements also affect consumer protection but instead should include noncompetition effects in their balancing of costs and benefits.
3. Antitrust authorities should take action when companies achieve monopoly power by misleading consumers about their data-collection policies.
4. Competition law should look at privacy issues even if no competitive implications exist.⁵

As Commissioner Ohlhausen points out, the U.S. Supreme Court has used a series of cases to make it clear that the primary criterion for antitrust enforcement is economic efficiency.⁶ And this is how it should be. U.S. regulators cannot use their powers to address speculative threats to competition. They must present the courts with sufficient evidence to conclude that a merger would result in real harm to consumers. The European Commission faces similar restraints because companies can appeal its decisions in the courts. This rightly constrains the agencies' ability to adopt a different standard even if they wanted to.

It is, of course, true that some companies have tighter privacy policies than others. But consumers generally have a lax attitude toward privacy; they say they want more of it, but they voluntarily share a lot of personal information online and generally do not support websites that cost even a little more, even when they claim to have better privacy practices.⁷ So there is no evidence a robust demand for enhanced privacy is going unmet, nor is there evidence that consumers have been harmed by the data practices of major platform companies.

⁵ Maureen K. Ohlhausen and Alexander P. Okuliar, "Competition, Consumer Protection, and The Right [Approach] to Privacy," *Antitrust Law Journal* 80 (2015): 134–36. In rejecting attempts to incorporate privacy concerns into antitrust policy, the authors point to three major problems: 1) Antitrust deals with harm to competition, not to privacy harms; 2) Antitrust is concerned with market-wide effects whereas privacy policy focuses on the individual relationship between the company and the consumer; and 3) Antitrust remedies are inadequate to handle privacy concerns because companies can accomplish the same outcome through private contracts rather than a merger;

⁶ Ohlhausen and Okuliar, "Competition, Consumer Protection, and The Right [Approach] to Privacy, 141–43.

⁷ Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," *Information Technology & Innovation Foundation*, July 2018, <http://www2.itif.org/2018-trust-privacy.pdf>.

More significantly, consumer-protection agencies have sufficient powers to ensure that companies honor any pledges they make about their data policies and comply with existing privacy regulations. They also have broad authority to address problems arising from the actual misuse of data. In the United States, a variety of laws protect privacy in specific market areas. Examples include the Children’s Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, and the Fair Credit Reporting Act. In the European Union, the protection of personal data is enshrined in the EU Charter of Fundamental Rights, and enforced via the ePrivacy directive and the General Data Protection Regulation (GDPR). These laws apply as much to data-rich tech giants as small start-ups. If policymakers are concerned with privacy, they are certainly capable of enacting stricter privacy laws as the EU has done, although if done improperly these regulations can have significant economic costs.⁸

Moreover, there is little evidence that providing users with more privacy gives a company a competitive advantage; otherwise more companies would be competing on this basis. So there is little reason to think that more competition on privacy would occur even if markets were perfectly competitive. From the company’s point of view, privacy restrictions limit possible data uses and therefore reduce revenues and the quality of service. And, despite what privacy advocates might wish, there is little evidence that consumers will pay an appreciable amount for restrictions on how their data can be used.⁹

The market for privacy is imperfect. Therefore, we should not expect it to solve all the privacy preferences of all users, since those preferences are so diverse. But this does not mean that decisions on antitrust issues should be driven by privacy concerns or that privacy laws are inadequate. There is no evidence that any lack of competition in providing services that feature greater privacy protections is due to entry barriers rather than a lack of consumer demand. Consumers may say they value privacy when surveyed, but the way they “vote with their clicks” suggests that they are more than satisfied with their current choices. Therefore, regulators should apply traditional competition analysis to the competitive aspects of a problem and use privacy laws to deal with privacy issues.

Privacy law relies heavily on the standard of informed consent to the use of personal data. But privacy advocates increasingly question the degree to which standard terms of use statements truly imply user

⁸ Daniel Castro and Alan McQuinn, “The Privacy Panic Cycle: A Guide to Public Fears About New Technologies” (Information Technology and Innovation Foundation, September 10, 2015), <https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies>.

⁹ Alistair R. Beresford, Dorthea Kübler, and Sören Preibusch, “Unwillingness to Pay for Privacy: A Field Experiment” (Social Science Research Center Berlin, June 2010), <http://ftp.iza.org/dp5017.pdf>.

consent.¹⁰ It is true that few users read these documents and that to use these services one has to agree to the company's policies. But that does not mean that the documents serve no purpose. First, they provide a record of how the company intends to collect and use data. This can subject companies to public scrutiny and criticisms by those who think they are unfair. Unfortunately, the threat of legal action can motivate the company to draft extremely comprehensive terms that incorporate any possible future uses it might imagine. This makes it difficult for users to understand which uses are actually likely. Nevertheless, the terms of use can create a market for more private services by allowing private groups to study them and inform consumers about their contents and whether any abuses have occurred.

Second, these agreements serve as terms of the contract between the company and the users. Regulators have taken action against companies for violating their own terms.¹¹

Third, it is hard to see any other alternative. Contracts of adhesion are widely accepted in many markets because they reduce transaction costs, especially in instances where it would be impractical to negotiate with every user or provide a menu of alternatives. Perhaps most important, the terms of use do not prevent legislators or privacy regulators from enacting binding laws on how companies protect and use data, irrespective of what the terms of use say. The main reason that this rarely happens is because there have been relatively few instances of companies engaging in clearly inappropriate behavior, and those have been handled by narrow disciplinary actions rather than broad regulation. Since Internet platforms have few valuable assets other than their brand and user base, they have an incentive to build a reputation for trust. This does not always overcome the temptations of profit or secrecy, but that is true for every industry. Past experience shows that users are willing to punish companies that misuse their data.¹²

Finally, any discussion of data and privacy has to recognize that there is no free lunch. Restrictive data policies reduce the economic value of data, and that means less revenues will be available for firms that rely on data for

¹⁰ Stucke and Grunes, *Big Data and Competition Policy*, 326–27, “The consensus is that the current notice-and-consent regiment [sic] is inadequate to safeguard privacy. Individuals are generally unaware who has access to their personal information, what data is being used, how the data is being used, when the data is used, and the privacy implications of the data's use.”

¹¹ Lisa Kimmel and Janis Kestenbaum, “What's Up With WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets,” *Antitrust*, Fall 2014, 49, (citing both the Nielson Holdings/Arbitron and Reuters/Thompson mergers), <https://www.crowell.com/files/Whats-Up-WithWhatsApp.pdf>

¹² Laura M. Holson, “To Delete or Not to Delete: That's the Uber Question,” *The New York Times*, November 21, 2014, <http://www.nytimes.com/2014/11/23/fashion/uber-delete-emil-michaelscandal.html>.

their business model. The result is either that free services will no longer be free, or that companies will have less resources to continue to innovate and improve the customer experience.

Sincerely,

Rob Atkinson
President, Information Technology and Innovation Foundation

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Doug Brake
Director, Broadband and Spectrum Policy, Information Technology and Innovation Foundation

Joe Kennedy
Senior Fellow, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation

Josh New
Senior Policy Analyst, ITIF's Center for Data Innovation