Before the
Federal Trade Commission
Washington, DC 20580

In the matter of Competition and Consumer Protection in the 21st Century Hearings	Project Number P181201

COMMENTS OF PUBLIC KNOWLEDGE

4. The intersection between privacy, big data, and competition. [1]

Consumer protection, fairness, and competition policy in today's digital economy require substantially stronger enforcement of antitrust law, more aggressive use of existing regulatory powers and new laws to fill in important policy gaps. Public Knowledge commends the FTC for launching this proceeding and a series of public hearings to examine competition and consumer protection in the 21st century, and today offers some initial observations and ideas to consider on the topics the Commission has identified as central to its inquiry. We will augment these ideas through our participation in Commission workshops and through follow up filings as the Commission refines the focus of its efforts.

The recent explosion in internet distribution of goods and services, growing dependence of democratic processes on nondiscriminatory and open digital communications platforms, and ongoing market dominance of entrenched media and communications companies makes it imperative for the FTC to become more vigilant and assertive to protect incipient and potential competition, to apply all qualitatively relevant elements to its consumer welfare analysis, and to update its consumer protection enforcement to reflect the complexities of the digital marketplace. As an expert agency with a specific mandate from Congress, it is also important for the FTC to inform lawmakers and the public of market imperfections and problems it lacks the tools and resources to address

[1] Public Knowledge staff John Bergmayer, Allie Bohm, Ryan Clough, Harold Feld, Meredith Rose, Kory Gaines, Dylan Gilbert, and Gus Rossi contributed to the comments filed in this proceeding.

and to propose policy adjustments that would more effectively address inequities in the oversight of today's economy.

Today, we are highlighting a number of the complexities and issues regarding application of FTC authority to the digital economy and the exploding internet economy in response to the Commission's request for comment. Rather than delineate precisely what deserves treatment under antitrust, consumer protection or some new legal authority, we instead highlight many of the problems that deserve careful attention, definition, further analysis and refinement before precise policy action should be considered. We offer this as a first step because we believe:

- the explosion of the digital market calls first for understanding precisely what is going wrong and therefore deserves fixing;
- identifying what are the best policy tools available to fix the problems;
- evaluating how best to apply existing policy tools; and
- proposing new policy tools to address problems that fall between the gaps under existing law.

This document contains our comments relating to intersection between privacy, big data, and competition.

We look forward to working with the FTC and all other stakeholders to flesh out the details of the concerns raised in our comments and propose meaningful policy adjustments and enforcement practices to help the Commission fully protect competition and consumers in the digital marketplace.

* * *

It has become virtually impossible to meaningfully participate in society without revealing our personal data. Most essential, entertaining, and useful internet services demand personal data that are used to build detailed user profiles and deliver targeted advertisements. Service providers follow us around the internet and across devices to show us ads, to collect more data, and to come up with more precise ways to sell us products. Credit rating agencies and financial institutions determine our access to mortgages and car loans based on the data they relentlessly collect from as many sources as possible. Employers use the amassed data to keep older workers from seeing certain job

postings,[2] and landlords use data to prevent racial minorities from accessing certain housing advertisements.[3] Pervasive data collection – and the decisions based on those data – may disproportionately harm historically disadvantaged communities. As our colleagues at the Center on Privacy and Technology at Georgetown University Law Center observe, black and brown people tend to over-index on social media platforms, and they, along with low-income people and teenagers, tend to disproportionately rely on smartphones for internet access, making them more susceptible to data collection and harmful biases in targeted advertising and algorithmic decision making.[4]

Many consumers are unsatisfied with this state of affairs. Some find it abusive that their privacy is the price of admission to socially or economically unavoidable internet platforms. Others hate to be paying twice for their internet service – both with their money and with their personal information. And nearly all are outraged by data breaches, hacks, revelations of corporate and state surveillance, and other social and political scandals. Consumers in the United States want more control over their personal data, and they demand privacy protection.

Many solutions have been proposed to defend consumers' privacy. The proponents of antitrust as a privacy remedy provide a variety of, often interrelated, rationales for this approach.[5] One is that dominant platforms impose abusive terms on their users who have no real option to leave the service, because network effects effectively lock them in. Another rationale is that antitrust safeguards consumer welfare by promoting consumer choice, and that antitrust enforcement should guarantee nonprice competition over different levels of privacy protection.[6] A third rationale suggests that companies should be held accountable under antitrust law when they mislead or deceive consumers about the

---

[2] Julia Angwin, Noam Scheiber, & Ariana Tobin, *Facebook Job Ads Raise Concerns About Age Discrimination*, NYTIMES, Dec. 20, 2017, https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html.
[3] Julia Angwin, Ariana Tobin, & Madeleine Varner, *Facebook (Still) Letting Housing Adertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017, https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.
[4] Center on Privacy & Technology et. al, Comment Letter on Competition and Consumer Protection in the 21st Century at 5 (Aug. 20, 2018).
[5] Allen P Grunes and Maurice E Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2600051 <https://papers.ssrn.com/abstract=2600051> accessed 29 June 2018.
[6] Robert H Lande, 'The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern'.

data collection practices that helped them achieve monopoly power.[7] And finally, there are those who believe that the possession of personal data is a potential barrier to future competition that should be considered during merger review, even when a merger would not otherwise have significant vertical or horizontal competitive effects.[8]

The above arguments show that antitrust has an important but narrow role in privacy protection. We agree that antitrust should encourage nonprice competition, including different levels of privacy protection, and that antitrust can be the right tool to fight anti-competitive hoarding of personal data. However, antitrust in general is not the right tool to address, nor the right conceptual framework to analyze, privacy harms in a comprehensive way.

There are three reasons why antitrust's role in privacy protection should be limited and narrow: 1) advocating for antitrust action requires a significant investment of political energy and time that has a very uncertain and unclear return for privacy protection; 2) antitrust action can have negative unintended consequences in the absence of an underpinning comprehensive privacy law, such as turning one privacy offender monopolist into several privacy offender competitors; and 3) antitrust cannot remedy most harms caused by non-dominant players.

First, antitrust cases consume significant amounts of regulators' limited political energy, time, and financial resources in exchange for, at most, a vague possibility of increased privacy protection. According to the Dechert Antitrust Merger Investigation Timing Tracker, on average a significant antitrust merger investigation in the US took 10 months in 2017.[9] The most relevant cases against dominant companies implicating consumer privacy tend to take even longer: United States v. Microsoft took over six years to be settled.[10] In Europe, the Google Search case has been open since 2010 and it is still

---

[7] Maureen K Ohlhausen and Alexander Okuliar, 'Competition, Consumer Protection, and the Right (Approach) to Privacy' (2015) 80 Antitrust Law Journal 121, 135.
[8] ibid 136.
[9] Dechert LLP, 'DAMITT: How Long Does It Take to Conduct Significant U.S. Antitrust Merger Investigations?' (July 2018) <https://www.dechert.com/knowledge/hot-topic/damitt--how-long-does-it-take-to-conduct-significant-u-s--antitr.html> accessed 19 July 2018.
[10] Antonio García Martínez, 'What Microsoft's Antitrust Case Teaches Us About Silicon Valley' [2018] *Wired* <https://www.wired.com/story/what-microsofts-antitrust-case-teaches-us-about-silicon-valley/> accessed 19 July 2018.

subject to litigation. Simply put, the return on investment of relying on antitrust to protect consumer privacy is non-optimal.[11]

Nor is it the case, as some maintain, that the expense of antitrust is reduced because many mergers are completed pursuant to settlement agreements and consent decrees that may include specific conditions to protect privacy. Not only are merger reviews time and resource intensive, but they require the relevant competition agency to invest adequate resources in ongoing enforcement. Settlement, or a consent decree as part of a merger approval, can only be a primary tool for protecting privacy if thoroughly enforced on an ongoing basis.

Second, in the absence of an underlying comprehensive privacy law, using antitrust to protect privacy could trigger many unintended consequences. Privacy advocates might find that using antitrust as a remedy backfires if, for example, the result of an antitrust action against a privacy-harming company is divided into several privacy-harming companies, none with sufficient market power to be considered dominant. Competition may create incentives to differentiate by providing greater privacy protection, but could just as easily promote more intense efforts to obtain more personal data as a competitive edge.

Third, the individual harms from a privacy violation can be the same regardless of the size of the company involved. Non-dominant companies that escape most antitrust scrutiny can harm an individual as much as dominant players. Although antitrust focuses on dominant companies and specific behaviors, such as collusion, companies of all sizes and in all types of markets commit privacy abuses every day. Given the importance of privacy for people's dignity, political organization, and social life, the protection of personal data should be a goal in and of itself, standing independently of competition policy.

A comprehensive approach to consumer protection is needed to deal with the many challenges presented by dominance in internet and telecommunication platforms and pervasive data collection practices. Policy-makers' and regulators' choice of policy tools

---

[11] European Commission, 'Summary of Commission Decision of 27 June 2017 Relating to a Proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement' <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018XC0112(01)&from=EN> accessed 19 July 2018.

should be guided by their intended policy goals and not vice-versa. Consumer protection requires accountability and fairness in markets. This includes tools to promote competition, consumer protection, privacy protection, diversity of information, and other public interest values.

What antitrust can do and its limits.

Calls to revive antitrust enforcement in the U.S., particularly in the digital communications and internet industries, are long overdue in light of evidence of increasingly concentrated markets and broader dangers to society such as privacy invasions and data breaches. However, these concerns are often presented in too simplistic a manner. While it is possible that, in theory, some idealized version of antitrust enforcement might resolve all competitive issues as well as the unintended and undesirable consequences of commercial processing and collection of personal data, neither current antitrust jurisprudence nor contemporary economic analysis supports this vision in practice.[12]

Antitrust analysis tends to be backward-looking, involving observed market outcomes judged to be the result of insufficient competition, leading to consumer harm. Structure is examined as the context that makes the conclusions about conduct more plausible. The lack of competition due to high levels of concentration, for example, may make it more likely that dominant platforms will be able to demand more personal data in order to sell more advertisements, but enforcement is triggered only when abuses can be demonstrated. This means that privacy advocates would have to demonstrate, within the existing parameters of antitrust law and practice, that a company is forcing consumers to agree to hand over their personal data in ways that distort competition.[13]

Antitrust reviews of corporate mergers reverse this analytical flow because it is the one area where antitrust is forward-looking. That is because structural analysis is central to the complaint that a merger will so greatly increase market concentration as to threaten consumers and competition.

---

[12] Gene Kimmelman and Mark Cooper, 'A Communications Oligopoly on Steroids - Why Antitrust Enforcement and Regulatory Oversight in Digital Communications Matter'.
[13] ibid.

In both ex post enforcement and merger review, however, the antitrust authorities often prefer structural remedies such as divestiture of assets to shrink market power, rather than remedies that require them to regulate the conduct of companies in the marketplace on an ongoing basis. This means that market structure, conduct, and performance are focal points, yet basic market conditions receive less attention. In fact, antitrust enforcers do not generally address basic market conditions because they are beyond their legal mandate. In the case of privacy protection, it is unlikely that an antitrust authority will be capable of creating and enforcing generic behavioral requirements to protect consumers' privacy.

Some characteristics of an industry make it unlikely that private investment and market forces will produce socially optimal outcomes. In some cases, investors cannot project or capture the benefits of the production of a common good, such as developing strong cybersecurity practices that protect personal data but might be costly to adopt for one actor if other actors are not following suit. In other cases, consumers cannot project the benefits of more output, such as a so-called network effect, which makes the network more valuable to consumers, who can reach more people, and to marketers, who can identify niches to expand output. These and other basic market attributes may not influence antitrust enforcers one way or the other unless a particular company acts abusively as it takes advantage of network effects.

Today, amidst calls to strengthen the antitrust oversight over digital platforms, it is important to remember that even in its "golden age" of trust busting in the first half of the 20th century, antitrust was never seen as enough on its own.[14] To the contrary, the same time period also saw the first wave of comprehensive consumer protection law to supplement antitrust. Louis Brandeis's arguments for creating the Federal Trade Commission emphasized the need for additional authority to protect consumers as a supplement to antitrust. Perhaps even more telling, Brandeis wrote his seminal article "The Right To Privacy" in the same year the Sherman Act passed.

Indeed, history has demonstrated that antitrust has periods of rigorous enforcement followed by periods of lax enforcement and concomitant reconsolidation. In these periods

[14] ibid.

when antitrust is less rigorously enforced, strong privacy protections become even more critical.

Why privacy is not only a market power issue

In 2013, Target announced that the personally identifiable information of 70 million of its customers had been compromised. Even assuming that Target has significant market power, it is difficult to see how antitrust could deal with harms of this sort. Single-firm conduct is typically only a violation of antitrust law to the extent that it unreasonably restrains competition; despite antitrust's focus on consumer welfare, it will not typically address negligent or risky behavior by dominant firms, even when such behavior harms consumers. But even this is beside the point, because Target does not likely have enough market power to sustain an antitrust action.

Few would argue that there is less of an obligation to protect the privacy of users of non-dominant platforms—or even of comparatively small platforms—than there is to protect the privacy of users of dominant platforms or that the harms suffered by the consumers of one are less than those suffered by consumers of others. If a small, non-dominant social network shares a person's health status with third parties without meaningful consent, the resulting risks of work, social, or healthcare discrimination would be as great as if they came from a dominant platform. The consequences of discrimination and the limitations to user autonomy based on the disclosure of delicate personal information are the same regardless of the size of the company that violated the trust of the consumer.

Principles for Effective Comprehensive Consumer Privacy Regulation.

Given the limits of antitrust enforcement as a tool to protect consumer privacy, the FTC must seek greater authority from Congress to protect consumers in the digital age. Any comprehensive privacy legislation should reflect the following:

Consumers deserve the right control the use of their personal information. At a minimum, consumers should have a right to know a) what information is being collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that

information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry recognized best practices.

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[15] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand. The FTC has already, in Agreements Containing Consent Orders, required that important terms be disclosed clearly and prominently and "separate and apart from any 'privacy policy,' 'data use policy, 'statement of rights and responsibilities,' or other similar document."[16] The FTC should encourage Congress to codify this best practice.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, and sharing. And, that consent should be as granular as possible. For example, a consumer should be able to consent for her data to be used for research purposes, but not for targeted advertising—or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so

---

[15] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[16] *E.g.* Facebook, Inc., 092 3184 (FTC, 2011).

desire. In addition, service should not be contingent on the sharing of data that is not necessary to render the service.[17]

Mandate data security. Those who collect and store this personal information have a duty to protect it. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society. When a breach of this trust occurs, the party that failed to properly secure the information should make the individual whole to the greatest extent possible.

Relatedly, organizations should be required to adhere to privacy by design and by default and to practice data minimization. The presumption should be that only data necessary for the requested transaction will be collected, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated.

End the sensitive/non-sensitive distinction. This distinction, which is used by the FTC and grants greater protection to purportedly sensitive information, like first and last name, social security numbers, bank account numbers, than to so-called non-sensitive information, is increasingly illogical in today's world. Indeed, pursuant to this distinction, information that may be useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and that, when aggregated, may, in fact, be personally identifiable would not be considered sensitive and would not be protected. It is time to confine the sensitive/non-sensitive distinction to the dustbins of history.

Americans need more privacy protection. Industry lobbyists have long sought to include federal preemption of state privacy and data breach laws as part of any new federal

[17] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

legislation. To the extent federal preemption is necessary to create a manageable national framework, it should be narrowly tailored to meet specific concerns.

Backward compatibility with existing federal privacy and data breach protections. The United States has relatively few federal statutes that directly impose privacy protections on industries. But while few in number, these laws form the basis for consumer privacy protection in critical industries such as health, communications, and financial protection. New federal protections for consumers should be "backward compatible" with existing protections.

Conclusion

The nexus between accumulated personal information and the dominance of internet platforms is properly within the scope of antitrust review, and antitrust enforcement to remedy anticompetitive uses of personal information can, and should, also strive to maximize consumer welfare in privacy. Similarly, it is appropriate for antitrust law to recognize that one of the harms of market dominance may be the power to coerce consumers into providing personal information in return for either "essential" or "unavoidable" services.[18] But these valuable roles for antitrust in the protection of privacy should not obscure the importance of stand-alone privacy regulation or the limitations of antitrust as a consumer protection tool. The FTC should strive to use antitrust law, where it can, to protect consumer privacy, but it must also advocate for comprehensive privacy legislation to truly protect consumers' privacy in the digital age.

Advocacy and policy change efforts should be driven by policy goals, and not by our attachment to particular tools. Antitrust should, in sum, be part of the toolkit necessary to protect consumer privacy. But we would do a disservice to consumers and privacy if we rely solely on antitrust for their protection.

Respectfully submitted,
Public Knowledge
August 20, 2018

[18] Laura Moy, Statement of Laura Moy, Deputy Director Center on Privacy & Technology at Georgetown Law 2018.