

Federal Trade Commission
Via Online Submission
Competition and Consumer Protection in the 21st Century Hearings, Project Number
P181201

August 10, 2018

FTC Commissioners and Staff:

As the Director of Consumer Privacy at the Center for Internet and Society at Stanford Law School, I thank you for the opportunity to submit comments to the Commission on the topic of privacy, big data, and competition. As a researcher with nearly 15 years' experience examining issues related to consumer privacy, I am pleased to see the Commission's interest in this topic. These comments address several sub-topics in Item 4: *The intersection between privacy, big data, and competition*.

My comments are based on my dissertation research, which I recently completed at the University of California, Berkeley School of Information, receiving my Ph.D in information management and systems in May 2018.¹ The portion of my dissertation research that I rely upon in these comments consisted of twenty qualitative interviews with ten users of free pregnancy tracking applications and ten users of the paid direct-to-consumer genetic testing service 23andMe. Across all twenty users, I asked questions regarding their use of free online search engine services. I asked participants specific questions regarding: their expectation of privacy when using these services; their willingness to pay for services that were presently free; what they would expect if switching to a paid service from a free version; what assurances (laws, third party guarantees, and similar) they relied upon when deciding to disclose personal information to these companies; the benefits they gained from their

¹ While this research has been reviewed and approved by my dissertation committee, I have not yet published it in a peer-reviewed venue. The dissertation itself can be accessed at:
http://www.jenking.net/files/jennifer_king_dissertation_final.pdf.

use of these services; what they thought the companies gained from their use of these products; and other questions related to their general use and trust in these products and services.

My research suggests the following about consumers and the intersection between privacy, big data, and competition:

- Lacking substantive negotiation power during the consent process, consumers often engage with companies even if their practices don't meet their privacy expectations. As a result, many consumers engage in strategies that they believe minimize their information exposure.
- Privacy policies do not present consumers with a useful means to compare competition on the basis of privacy.
- Some consumers are willing to 'pay for privacy'—pay for products or services that were previously offered at no charge—assuming there are explicit benefits for the consumer, especially restrictions on the collection, use, and sale of personal data.
- A lack of regulation creates incentives for companies to collect as much information as possible about consumers, rather than compete on the basis of privacy.
- Many consumers appear to be confused about privacy laws and/or misinformed about the functional purpose of privacy policies. As a result, the basis by which consumers choose to disclose their personal information to companies is flawed and potentially puts them at greater risk than they would prefer.

I address these issues and more below.

Issue 1: Comment on “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.”

American consumers do care about information privacy. My own and others' nationally representative survey work have chronicled this fact for over a decade.² Despite this demonstrated concern, some argue that because consumers continue to use products and services that pose them privacy risks, their actions reveal that consumers don't actually care about privacy. Others attempt to explain this

² See generally: Turow, Joseph and King, Jennifer and Hoofnagle, Chris Jay and Bleakley, Amy and Hennessy, Michael. Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). Available at SSRN: <https://ssrn.com/abstract=1478214>; and Hoofnagle, Chris; King, Jennifer; Li, Su; and Turow, Joseph. How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies (2010)? Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

divergence by arguing for the existence of a privacy paradox: that while consumers do care about their privacy, there are multiple mediating factors that explain why consumers act as if they do not.

My own research in this area suggests additional interpretations:

- In most instances, consumers who adopt a new product or service have little choice beyond agreeing to a ‘take it or leave it’ consent regime. While they may have privacy concerns about a product or service, they have no meaningful negotiation power in the consent process other than opting to not adopt the service. Thus, consumers often agree to the terms a company offers even while actively harboring privacy concerns because they see no other option.
- In the absence of comparative alternatives to a product or service (particularly those services that currently have monopoly or near monopoly power in the marketplace), privacy concerned consumers will engage in strategies to minimize their exposure to a company in order to exert some level of control over the collection and use of personal information. Strategies include: falsifying some personal information; using private browsing; using ad blockers; or electing to not provide information when optional.
- Insofar as a company’s data use policies are presented only in a formal privacy policy, consumers will not use that information for comparison purposes. The vast majority of privacy policies do not present information in a format that most consumers can understand, let alone parse and create meaningful comparisons.
- Companies often present generic privacy policies that do not address the data collection and use practices of specific services, such as a company’s mobile app. In many instances, a consumer seeking information about an app’s or a specific product’s data collection practices won’t find it. Instead, she will be routed to a privacy policy for a company’s website, which may not contain any detail about specific products or services.³

Currently, there are few, if any incentives for companies to meaningfully compete on privacy. Lacking any restrictions on information collection, many companies are engaged in a race to the bottom to aggregate as much data as possible in the event that customer data can be monetized or reused in a way not foreseen at the time of collection. Given that there are greater incentives for companies to collect as much information about consumers as possible rather than minimize

³ For an example, please see the privacy policy for Amazon.com, located at: https://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496. As of August 2018, this privacy policy relates only to Amazon.com and contained no specifics about the information collected by Amazon mobile applications, tablets, voice assistants, or smart speaker systems.

collection, baseline restrictions on collection and reuse of personal information would help rein in these practices. Further, there are presently no regulations that attempt to standardize data use policies in format, content, risk assessment, or terminology. Without a standardized method for comparing companies' data use, it is both unclear how companies can meaningfully compete on privacy attributes and how consumers would evaluate them. Without this data, consumers will continue to evaluate companies based on heuristics and other trust signals that help them divine how trustworthy a company might be with their personal data.

Issue 2: Comment on “whether consumers prefer free/ad-supported products to products offering similar services or capabilities but that are neither free nor ad-supported.

In my dissertation research, I explicitly asked a set of twenty research participants questions regarding their use of a set of free products that required an exchange of personal data for access to the service. I posed questions such as: Would they be willing to pay for a service they presently receive for free? If they paid, what expectations did they have regarding any differences in how their data would be collected or used? My findings are summarized as follows:

- Some consumers are willing to ‘pay for privacy’ and would forgo a free service for a paid service if paying for the service meant their personal information would not be shared, sold, or used in ways in which they did not explicitly consent.
- Most participants in my study expressed an expectation that the trade-offs for a paid product would be explicit and to their benefit, such as: no ads, no ad targeting, expanded features not available in the free service, and responsive customer service.
- Switching costs and lock-in were seen as major impediments to adopting any new service. This was particularly evident in platforms such as Google, where participants’ use of multiple Google services made them less motivated to switch to a different search engine with more explicit privacy guarantees.
- The direct benefit that consumers receive from a company matters in these calculations. To some extent, it is difficult to discuss this topic in the abstract as the substantive benefit a consumer obtains varies widely, as do consumer expectations on this topic, and the benefit a consumer obtains from a product may directly compete with one’s concerns about privacy. For example, in my research study the participants voiced reluctance to pay for a previously

free product unless it was supplemented, as described above, with enhanced features or explicit restrictions on the collection and use of their personal data.

In sum, my research has found that in some contexts, consumers voice a willingness to pay for an ad-free service as long as there are explicit privacy benefits to be gained. However, the proposition has to have a clear value proposition to the consumer; there are potentially some products and services where either consumers simply don't see enough of a benefit to justify the payment, or the true cost to them—the collection and use of their personal information in ways in which they do not understand or are unaware of—is hidden.

Issue 3: Comment on “the benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection.”

As I note in my response to Issue One, our largely unregulated marketplace in personal information encourages a race to the bottom by companies on privacy and data use, disincentivizing companies from competing on features that provide consumers with additional privacy protection. It is also important to note that today many consumers are both *uninformed and misinformed* about the lack of privacy regulation governing data use by companies, especially in the technology sector.

In 2009, my colleagues and I published survey findings where we discovered a significant level of misinformation about the basics of privacy policies.⁴ My recent research bolsters these findings and uncovers little substantive change over the years: many consumers are still confused or misinformed about the functional purpose of privacy policies (including, most disturbingly, the assumption that having a privacy policy *means* that a company protects individual privacy). To some extent, this misinformation may also emanate from the term “privacy policy” itself, which consumers appear to interpret to mean that *by definition* the policy protects one's privacy.

When I asked my dissertation research participants what assurances (laws, third party guarantees, and similar) they relied upon when making disclosure decisions, most suggested a range of non-legal factors, such as: a company's reputation; friend and family referrals; and visual website heuristics, such as the look and feel of a company's website. Legal assurances, such as specific laws or the

⁴ Turow *et al.* in *supra* 2.

ability to engage in a civil action (class action or independently) were not top of mind. Consumers demonstrate confusion by assuming laws exist to protect their privacy where none actually do. In some cases, this is a result of misapplying an existing privacy law outside of its actual context (e.g., assuming a pregnancy app, because it tracks health-related data, is covered by HIPPA). In others it is a result of misinformation, in some instances again relying on the overloaded concept of privacy policies.

I bring these findings to the Commission's attention because while implementing laws that place restrictions on the collection, use, and sale of personal information may benefit consumer privacy, it is important to note that today that evidence suggests that many disclosure decisions are driven by a fundamental misunderstanding by consumers about what laws actually exist. Some companies benefit from consumer confusion and misinformation by attracting customers that might otherwise find their privacy practices objectionable. These findings should not be interpreted as obviating the need for regulation, but instead highlight the fact that the extant notice and choice framework fails to properly inform consumers, and as a result, consumers make uninformed choices, disclosing personal information in circumstances that may make them vulnerable beyond what they would wish to tolerate if they had a full understanding. Subsequently, stronger consumer privacy protections would aid a class of consumers who are today unwittingly putting themselves at potential risk.

Thank you for the opportunity to comment on these issues.

Sincerely,

Jennifer King, Ph.D

Director of Consumer Privacy
Center for Internet and Society
Stanford Law School