



THE ADVOCACY DIVISION OF CONSUMER REPORTS

August 20, 2018

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 P1812201

4. The intersection between privacy, big data, and competition;

Antitrust

For Consumers Union's comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

Consumers Union¹ strongly supports the enactment of comprehensive privacy and security legislation as the commercial and societal benefits significantly outweigh any costs. First, for security, the Federal Trade Commission (FTC) has already used Section 5 of the FTC Act extensively to punish unreasonable data and cyber security practices. Legal accountability is important, because companies who fail to safeguard their products and services do not bear the direct risks from resulting security incidents; a company may anticipate that it could one day bear some loss to goodwill or reputation, though that risk is discounted by its occurrence in the (possibly distant) future, and attribution for data breaches is notoriously difficult. And this assumes perfectly rational company decision-making, whereas in reality companies tend to underestimate the potential losses posed by tail-risk events, and are often overly incentivized for focus on short-term revenues. Security law should require companies to internalize the potential harm to the ecosystem

¹ Consumers Union is the advocacy division of Consumer Reports, an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumers Union works for pro-consumer policies in the areas of antitrust and competition policy, privacy and data security, financial services and marketplace practices, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

in their product planning and development, though no system need strive for *perfect* security—instead, companies should take reasonable and appropriate measures that take into account potential threat models, sensitivity of information, and also the cost of particular security measures.

With regard to privacy, legislation should seek to empower individuals to make choices about the collection and use of their personal information, and to align business practices with reasonable consumer expectations. Today many data practices are completely intransparent to consumers, leaving them generally frustrated but ultimately incapable of making informed choices.² Many consumers may willingly accept advertising-support products, but far fewer understand or agree to cross-service data tracking;³ due to lack of information, companies are able to free-ride on consumers' data without accountability. Privacy disclosures are currently not designed to convey meaningful information either to ordinary consumers or even sophisticated privacy analysts. At the very least, companies should be required to provide more precise information to the market, whether through consumer-facing disclosures or in detailed policies more suited to regulators, press, and analysts. Consumers should be able to obtain access to the information that companies have about them in a structured format to promote accountability and competition. Privacy law should also provide some limitations or choices around the secondary use or retention of data, though even advocates disagree on when outright prohibitions, or either opt-in or opt-out choices, are appropriate. All have their limitations: prohibitions may be too blunt, opt-in requirements can be gamed through the use of coercive dark patterns by companies with few competitors,⁴ and opt-out choices are difficult to scale. However, given the rapid advance of technology, the alternative of doing nothing is still worse: companies increasingly possess the capacity to collect, store, and process every piece of data about us. Certainly it cannot be the case that consumers must passively

² A Mozilla study found that a third of people feel like they have no control of their information online. *Hackers, Trackers, and Snoops: Our Privacy Survey Results*, MOZILLA (Mar. 9, 2017), <https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5>. And although the majority of consumers (74%) find it is “very important” to be in control of who can get information about them. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>. A Pew research poll found that 91 percent of adults “‘agree’ or ‘strongly agree’ that consumers have lost control over how personal information is collected and used by companies.” Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

³ Chris Kahn & David Ingram, *Americans Less Likely to Trust Facebook than Rivals on Personal Data*, *Reuters/Ipsos Poll*, REUTERS (Mar. 25, 2018)<https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3>; Joseph Turow, *et al.*, *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN (Sept. 29, 2009), <https://ssrn.com/abstract=1478214..>

⁴ DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY, NORWEGIAN CONSUMERS COUNCIL (June 27, 2018), *available at* <https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/>; *and, see*, Allen St. John, *CR Researchers Find Facebook Privacy Settings Maximize Data Collection*, CONSUMER REPORTS (June 27, 2018), <https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/>; *CU Letter to FTC on Norwegian Consumer Council Report “Deceived by Design” and CU Research on Facebook and Google Sign-Up*, CONSUMERS UNION (June 27, 2018), <https://consumersunion.org/research/letter-to-ftc-norwegian-consumer-council-report-deceived-by-design/>.

submit to boundary-less surveillance simply in order to facilitate a never-ending flow of relevant offers.

Contrary to industry talking points, privacy regulation will benefit *consumers*, not Google and Facebook, which have lobbied aggressively against any expansion of privacy law both in the United States and Europe.⁵ Indeed, Google and Facebook are *already* over-powerful and outsized monopolies absent new privacy rules. Similar arguments about the balance of benefits between consumers and those companies were advanced against the Commission's call for a Do Not Track (DNT) browser control;⁶ again, however, both fought hard to stop industry adherence to that standard. As a result, Google and Facebook (and the vast majority of the ad tech industry) ignore users' DNT instructions on the web to this day.

Certainly, if a company's business model is predicated entirely on bad privacy practices, then privacy legislation will especially impact them, and will appropriately disadvantage them more compared to companies like Google and Facebook. Both companies have problematic practices that should be addressed by privacy rules, but both also have core products that can be monetized effectively without compromising user privacy. However, because those companies' business models are also heavily reliant on the use of personal information, privacy law does impact them directly—and more than most companies. The Commission has already brought actions against both companies for privacy violations, though due to weaknesses in the law and the limitations in its own authority, its actions have not sufficiently deterred their abuses.

To be clear, effective privacy law should not simply mandate expensive processes and compliance programs. Some companies have sought to frame privacy regulation in terms of *accountability*—a form of self-regulation prioritizing the development of internal policies and procedures over actual substantive rights and protections. A privacy regime that pairs high levels of process with weak substantive rules may in fact unduly favor large companies while doing little to actually preserve users' privacy. Fundamentally, privacy law should accord behaviors with the consumer's reasonable expectations; if a small business is not engaged in dubious data practices, it should not have to alter its practices as much as a larger player like Google or Facebook when complying with new privacy protections.

The continued erosion of privacy also adds to the existing imbalance of information and power between consumers and businesses. Data collection affords companies greater insight and leverage

⁵ Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit from Europe's Privacy Crackdown*, WALL ST. J. (Apr. 23, 2018), <https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324>; Daisuke Wakabayashi & Adam Satariano, *How Facebook and Google Could Benefit from the G.D.P.R., Europe's New Privacy Law*, N.Y. TIMES (Apr. 23, 2018), <https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html>.

⁶ *FTC Testifies on Do Not Track Legislation*, FED. TRADE COMM'N (Dec. 2, 2010), <https://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation>.

for negotiating individualized prices, allowing companies to extract relatively more of the consumer surplus out of any given transaction. Increased corporate concentration tied with unconstrained data collection and sharing is likely to lead to greater first-order price discrimination, leading to worse results for consumers and greater inequality. As such, consumers have a rational interest in limiting data collection separate from any demonstration of objective “injury.”

More broadly, privacy and competition are linked because it is considerably harder for individuals to make privacy-conscious choices when there are, in fact, no choices. While legal protections around privacy and security should be strengthened, there is also a role for improved marketplace solution. As discussed in more detail in our response to Topic 1, privacy policies and disclosures do not typically convey meaningful information to consumers upon which they can make reasoned choices. As such, Consumer Reports has started testing a range of products and services for elements such as privacy and security as part of our Digital Standard work.⁷ We recently published our first set of ratings under this project as part of a broader assessment of personal peer-to-peer payment applications.⁸ Increased market pressure due to improved transparency can help hold companies accountable for bad practices and bend corporate behaviors in a more positive direction for consumers. However, in the increasing number of markets insulated from sufficient competition, increased transparency can only have a more limited effect. For that reason, there is a rationale for stronger privacy rules for industries in concentrated sectors, such as internet service providers.⁹ More broadly, the Commission should reinvigorate its commitment under competition law to ensure that markets provide sufficient *consumer choices* in order to function effectively.

Respectfully submitted,

Justin Brookman
Director, Consumer Privacy
& Technology Policy

Consumers Union
1101 17th Street, NW

⁷ The Digital Standard (theDigitalStandard.org) was launched on March 6, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

⁸ Tobie Stanger, *Why Apple Pay is the Highest-Rated Peer-to-Peer Payment Service*, CONSUMER REPORTS (Aug. 6, 2018), <https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/>.

⁹ For more on this subject, please see Consumers Union’s response to Topic 2: *Competition and consumer protection issues in communication, information, and media technology networks*.

Suite 500
Washington, DC 20036