



**NEW YORK
LAW SCHOOL**

August 20, 2018

Mr. Donald S. Clark, Secretary
Federal Trade Commission
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 Mr. Clark,

The Advanced Communications Law & Policy Institute (ACLP) at New York Law School respectfully submits the following filing in response to the Commission's request for comment ahead of its hearings on Competition and Consumer Protection in the 21st Century.

The Commission is to be commended for spearheading this inquiry. The slate of questions and hearing topics identified by the Commission indicate a genuine desire to understand how best to protect consumers, preserve competition, and support continued innovation in the digital ecosystem.

The ACLP looks forward to serving as a resource to the Commission during the upcoming hearings. Should you have any questions, please do not hesitate to contact us.

Respectfully submitted,

/s/ Charles M. Davidson
CHARLES M. DAVIDSON, DIRECTOR

/s/ Michael J. Santorelli
MICHAEL J. SANTORELLI, DIRECTOR

To: Mr. David S. Clark, Secretary, Federal Trade Commission

From: Charles M. Davidson & Michael J. Santorelli, ACLP at New York Law School

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

Date: August 20, 2018

A. INTRODUCTION & EXECUTIVE SUMMARY

The FTC is to be commended for soliciting comments and convening hearings to study the impact of new digital technologies and business models on consumer welfare.

1. A Vastly Different Landscape

Much has changed since the Pitofsky Hearings were convened in 1995. At that time, only 14% of U.S. adults had Internet access,¹ and those who went online were largely indifferent to the web's offerings. In a survey of Internet users in 1995, it was observed that:

“Few see online activities as essential to them, and no single online feature, with the exception of E-Mail, is used with any regularity. Consumers have yet to begin purchasing goods and services online, and there is little indication that online news features are changing traditional news consumption patterns.”²

Today's landscape is vastly different.

- 89% of U.S. adults use the Internet.³
- 65% of U.S. adults have a home broadband connection.⁴

¹ See Susannah Fox & Lee Rainie, *The Web at 25 in the U.S. – Part 1: How the Internet Has Woven Itself into American Life*, Feb. 27, 2014, Pew Research Center, <http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/#fn-10743-4>.

² See *Americans Going Online...Explosive Growth, Uncertain Destinations*, Pew Research Center (Oct. 1995), <http://www.people-press.org/1995/10/16/americans-going-online-explosive-growth-uncertain-destinations/>.

³ See *Internet/Broadband Fact Sheet*, Feb. 5, 2018, Pew Research Center, <http://www.pewinternet.org/fact-sheet/internet-broadband/>.

⁴ *Id.*

- 20% of U.S. adults use a smartphone and mobile broadband connection as their primary or sole means of Internet access.⁵ (In 1995, only one in ten Americans used a cellphone.⁶)
- The average American Internet user spends almost 24 hours each week online, up from 9.4 hours a week in 2000.⁷
- It is projected that U.S. consumers will soon spend more time online than they will watching TV.⁸

2. Tech's Dark Underbelly

These data offer a small window into how deeply rooted into modern life technology is. But as headline after headline highlight, the downsides of constant connectivity are beginning to weigh on consumers and society at large. Indeed, beneath the Internet's shiny utopian surface lurks many untold dangers for consumers.

- Digital services are designed by their makers to be addictive.⁹ The addictions are taking root. Many users feel compelled to constantly check their smartphone, Twitter feed, or Facebook page. This addiction harms consumers (*e.g.*, by exponentially increasing stress and anxiety levels), while inuring to the benefit of the suppliers (*i.e.*, tech companies) in the form of higher revenues.¹⁰
- Constant connectivity results in consumers regularly exposing, often without notice or any real consent, ever more granular information about themselves while online. An array of actors of all ilk are constantly mining the Internet for consumers' views, demographic profiles, purchases,

⁵ *Id.*

⁶ *In re Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993*, First Report, 10 FCC Rcd. 8844, ¶ 6 (July 28, 1995).

⁷ See *Surveying the Digital Future*, at p. 5-6, Digital Future Project, Center for the Digital Future (2018), <https://www.digitalcenter.org/wp-content/uploads/2018/04/2017-Digital-Future-Report-2.pdf>.

⁸ See Rani Molla, *Next year, people will spend more time online than they will watching TV. That's a first.*, June 8, 2018, Recode, <https://www.recode.net/2018/6/8/17441288/internet-time-spent-tv-zenith-data-media>.

⁹ See, *e.g.*, Olivia Solon, *Ex-Facebook President Sean Parker: Site Made to Exploit Human 'Vulnerability'*, Nov. 9, 2017, The Guardian, <https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology>.

¹⁰ See, *e.g.*, Tim Bradshaw & Hannah Kuchler, *Smartphone Addiction: Big Tech's Balancing Act on Responsibility over Revenue*, July 23, 2018, Financial Times, <https://www.ft.com/content/24eeaed6-8a7f-1e8-b18d-0181731a0340>.

interests, contacts, browsing history.¹¹ The business practices of those that collect and monetize this data have been likened, appropriately, to Big Brother-esque surveillance.¹² This analogy is based on real-world examples of questionable behavior by these firms, which seem to come to light every week. The latest in the long line of such examples: “Google services on Android devices and iPhones store your location data even if you’ve used a privacy setting that says it will prevent Google from doing so.”¹³ In short, tech companies push and often exceed the boundaries of personal privacy in their drive to mine and commoditize our data.

- The data collected and monetized by online firms is increasingly being used to substantiate harmful outcomes for certain consumers. For example, people of color are at significant risk of suffering unjust discriminatory outcomes online as a result of algorithmic bias.¹⁴
- Notwithstanding that consumers’ online data is a precious resource for big tech, consumer data is constantly hacked and misused. The scandal involving Facebook and Cambridge Analytica, along with the untold data breaches that have been reported in recent years, underscore this vulnerability.¹⁵
- In terms of social discourse, rather than fostering collaboration and productive dialogue, the Internet has fueled partisanship, creating echo chambers that reinforce views and stoke conspiracy theories.¹⁶ The

¹¹ See, e.g., Michael Santorelli, *Halo, Goodbye: Cleaning Up the Digital Ecosystem After the Facebook Data Spill*, April 24, 2018, Forbes Washington Bytes, <https://www.forbes.com/sites/washingtonbytes/2018/04/24/halo-goodbye-cleaning-up-the-digital-ecosystem-after-the-facebook-data-spill/#3d7e00a31ueb> (“Halo, Goodbye”).

¹² The term “surveillance capitalism” was coined to describe the practices of tech firms like Google to “predict and modify human behavior as a means to produce revenue and market control.” See Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 *Journal of Information Technology* 75 (2015).

¹³ See Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Aug. 13, 2018, Associated Press, https://www.apnews.com/828aefab64d441bac257a07c1afoecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not?te=1&nl=dealbook&emc=edit_dk_20180813.

¹⁴ See, e.g., Joy Buolamwini, *When the Robot Doesn’t See Dark Skin*, June 21, 2018, N.Y. Times, <https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html>.

¹⁵ See, e.g., *Halo, Goodbye*.

¹⁶ See, e.g., David Dillard-Wright, *Technology Designed for Addiction*, Jan. 4, 2018, Psychology Today, <https://www.psychologytoday.com/us/blog/boundless/201801/technology-designed-addiction> (“The feedback loops of social media also drive political polarization and confirmation bias, as we are constantly pushed in the direction of content that aligns with what we already believe and fits with the demographic groups to which we already belong. As we get more and more used to the creep of technology into our lives, this comes to seem completely normal.”).

companies offering the platforms that fuel “fake news” and “trolling” profit as a result.

Consumer welfare in the digital ecosystem is on a precipice. The threats to consumer welfare are real, pervasive, enduring, and taking root in every facet of society. If policymakers fail to address these threats and inject some measure of order into the ecosystem, consumers will suffer – and the foundations of our democracy will erode. This is not hyperbole. One need only look to the roles that big tech – firms like Facebook, Google, Twitter, and their ilk – play in politics and public discourse to appreciate how influential these firms are in shaping public opinion and swaying elections.¹⁷ Consumers agree: according to a recent poll, “most Americans (55%) now say social media does more to hurt democracy and free speech than it helps.”¹⁸

3. Where Does the FTC Come In?

As the federal agency charged with “protect[ing] consumers by preventing anticompetitive, deceptive, and unfair business practices,” the Commission must play a lead role in policing bad behavior in the digital ecosystem.¹⁹ Indeed, the FTC possesses broad authority to play a more active role in protecting consumers from the invasive business practices of tech companies eager to profit from their personal information.²⁰ That authority must be strengthened by Congressional action to address data privacy more generally.²¹ But in the meantime, the Commission cannot be idle. It must act. Using the upcoming hearings as a jumping off point, the FTC must establish itself as a serious market-monitor and regulator of this space.

To these ends, the following guiding principles are offered to inform the Commission’s approach to the digital ecosystem going forward. As an overview, these principles include:

¹⁷ See, e.g., Fred Wertheimer & Norman Eisen, *What Facebook, Google, and Twitter Owe America*, Feb. 28, 2018, Politico Magazine, <https://www.politico.com/magazine/story/2018/02/28/what-facebook-google-and-twitter-owe-america-217096>.

¹⁸ See Kim Hart, *Exclusive: Public Wants Big Tech Regulated*, Feb. 28, 2018, Axios, <https://www.axios.com/axios-surveymonkey-public-wants-big-tech-regulated-5f60af4b-4faa-4f45-bc45-018c5d2b36of.html>.

¹⁹ See FTC, About the FTC, <https://www.ftc.gov/about-ftc>.

²⁰ Cf. *LabMD v. FTC*, No. 16-16270 (6th Cir. June 6, 2018).

²¹ See, e.g., Omar Tene, *Lessons from LabMD: Reading Between the Lines of FTC Decisions*, June 11, 2018, IAPP, <https://iapp.org/news/a/lessons-from-labmd-reading-between-the-lines-of-ftc-decisions-2/> (highlighting the need for federal legislation in an effort to delineate the scope of FTC authority to act vis-à-vis privacy and data security issues).

Principle #1: The FTC Must Play a More Collaborative & Active Role in Monitoring the Digital Ecosystem

Principle #2: The FTC Must Understand the Business Models, Practices & Incentives Driving Major Tech Firms in the Digital Ecosystem

Principle #3: The FTC Must Recognize & Operationalize the Foundational Fact that Market Power in the Digital Ecosystem Revolves Around Data

Principle #4: The FTC Should Make Clear that Enhanced Transparency is Essential to Bolstering Consumer Welfare in the Digital Ecosystem

Principle #5: The FTC Must Stake Out a Lead Role in Enforcement

B. GUIDING PRINCIPLES FOR FTC OVERSIGHT & ENFORCEMENT

1. The FTC Must Play a More Collaborative & Active Role in Monitoring the Digital Ecosystem

In the recent past, the Commission has not been as active as it could be in the context of policing the digital ecosystem and protecting consumers against harmful business practices.

- Relatively lax merger review has allowed big tech firms to become even larger and more dominant in the collection and monetization of consumer data.²²
- Enforcement actions in the context of online privacy have been piecemeal, amounting to more of a common law approach rather than the development of precedents and standards that can shape behavior going forward.²³ Similarly, the Commission “primarily relies upon theories of deception when alleging privacy violations,” which has resulted in the FTC “bring[ing] most of its privacy-related enforcement actions against companies that violate their own privacy policies or fail to disclose their data collection and use practices.” This approach is tantamount to a “do not

²² See, e.g., *American Tech Giants are Making Life Tough for Startups*, June 2, 2018, *The Economist*, <https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups>; Michael Santorelli, *Art of the Deal: Merger Mania in Trumpland?*, Aug. 2, 2017, *Forbes Washington Bytes*, <https://www.forbes.com/sites/washingtonbytes/2017/08/02/art-of-the-deal-merger-mania-in-trumpland/#56d385862407> (comparing and contrasting the relatively more robust antitrust review of recent telecom mergers with the relatively lax reviews of recent tech mergers).

²³ See, e.g., Daniel J. Solove & Woodrow Harzog, *The FTC and the New Common Law of Privacy*, 114 *Columbia L. Rev.* 583 (2014), <http://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf>

lie” rubric and does nothing to modify future behaviors.²⁴ Instead, this approach creates incentives for firms to be even more clandestine with respect to their data collection methods.²⁵

- There have been too few inquiries into potential anticompetitive activities of big tech. The Commission opened an investigation into Facebook’s actions vis-à-vis Cambridge Analytica,²⁶ but previous inquiries into allegations of anticompetitive conduct by firms like Google have either been closed or have resulted in outcomes (*i.e.*, consent decrees or fines) that have no meaningful effect on conduct in the tech ecosystem.²⁷ The FTC has ceded its role as the lead policeman on the privacy beat to antitrust authorities in Europe.²⁸

Reversing course in these and related areas appears to be a main objective of the hearings. The newly constituted Commission has signaled a desire to “prioritize, examine, and address privacy and data security with a fresh perspective.”²⁹ To that end, the Commission should view the hearings as a first step, not an end in itself. More specifically, in follow up to the hearings, the Commission must remain engaged with experts and should create pipelines through which insights, analysis, and recommendations from stakeholders can flow to the Commission.

In the past, the Commission has relied on workshops and other periodic gatherings as a way to gather this kind of input. As a supplement to these events, the FTC should explore the establishment of working groups, task forces, and similar initiatives that bring

²⁴ See WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 68 (2018).

²⁵ See, *e.g.*, CHRIS JAY HOOFNAGLE, *FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY* 352-354 (2016) (highlighting the consumer threats arising from the “bait and switch” practices of edge providers like Facebook and Google, wherein a “website...lures consumers with various free services or other promises but...later switches and adopts privacy-invasive practices” [citations omitted]).

²⁶ See *Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices*, March 26, 2018, FTC, <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>.

²⁷ See, *e.g.*, Ed Wyatt, *A Victory for Google as F.T.C. Takes No Formal Steps*, Jan. 3, 2013, N.Y. Times, <https://www.nytimes.com/2013/01/04/technology/google-agrees-to-changes-in-search-ending-us-antitrust-inquiry.html>.

²⁸ See, *e.g.*, Press Release, *Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service*, June 27, 2017, European Commission, http://europa.eu/rapid/press-release_IP-17-1784_en.htm; Press Release, *Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google’s search engine*, July 18, 2018, European Commission, http://europa.eu/rapid/press-release_IP-18-4581_en.htm.

²⁹ See *Statement of the FTC Before the Committee on Energy and Commerce*, at p. 6, July 18, 2018, FTC, https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf (“*Statement of the FTC*”).

together outside experts – academics, consumer advocates, industry executives, etc. – to explore and opine on discrete issues. The Commission should study the array of initiatives that the Federal Communications Commission (FCC) has launched in recent years, which have generated work product that has informed rulemakings and policymaking generally.³⁰ The use of such expert-driven working groups could create flows of information that mimic traditional notice-and-comment procedures that attend formal rulemaking, a power that the FTC unfortunately lacks.

2. The FTC Must Understand the Business Models, Practices & Incentives Driving Major Tech Firms in the Digital Ecosystem

Drawing on the expertise of stakeholders should be only a first step toward the Commission becoming more active in the digital ecosystem. Indeed, it will be essential for the FTC to undertake comprehensive inquiries into the mechanics of this space so that it fully understands (1) the players involved, (2) their business models, and (3) their motivations and incentives vis-à-vis data collection.

Unlike at any time in the past, the business models of modern communications and media firms are increasingly built around the collection and monetization of granular, real-time information detailing every aspect of online use.³¹ Indeed, this kind of data is the common thread linking together firms throughout the ecosystem.³² At a very basic level, it is central to what these various firms do: ISPs deliver data to consumers (they derive almost all of their revenue from voice, video, and data subscriptions); content producers create data for delivery to and consumption by consumers (these companies typically make money by placing ads based on these uses); and device manufacturers produce the hardware that consumers can use to access data (in many instances, these firms collect data, too). But in the context of discussions about privacy and competition policy, this simple schematic is ultimately misleading because it obscures a basic truth about the modern digital ecosystem: content firms across every segment are competing viciously to be the entity that controls how users' data are collected and monetized.³³

³⁰ See, e.g., FCC, Broadband Deployment Advisory Committee, <https://www.fcc.gov/broadband-deployment-advisory-committee>; FCC, Consumer Advisory Committee, <https://www.fcc.gov/consumer-advisory-committee>.

³¹ See, e.g., James Grimmelman, *The Structure of Search Engine Law*, 93 Iowa L. Rev. 1, 11-15 (2007) (discussing the role of data in enabling the business models of online search engines).

³² See, e.g., FRED VOGELSTEIN, *DOG FIGHT: HOW APPLE AND GOOGLE WENT TO WAR AND STARTED A REVOLUTION 183-202* (2013) (providing an example of how technological convergence is driving the race to position proprietary platforms like Apple's mobile devices as the primary arbiter of the online experience).

³³ See, e.g., Bryan Choi, *The Anonymous Internet*, 72 Maryland L. Rev. 501 (2013) (discussing the interplay between innovation – or “generativity” – and notions of privacy like anonymity and noting that the robustness of the former increasingly hinges on flexibility in the latter).

This general dynamic has been evident since the earliest days of the commercial Internet, when firms competed to serve as exclusive portals to Internet content. This “walled garden” approach, however, quickly fell out of favor as consumers took advantage of new tools to explore the World Wide Web.³⁴ The result was a remaking of the Internet ecosystem: “those who wanted to reach [consumers who were actively exploring the Web on their own], such as commercial merchants and advertising-driven content providers, found it easier to set up outposts [in cyberspace] than through negotiated gates of the proprietary services.”³⁵ Accordingly, online firms began to compete for market share in what was a burgeoning e-commerce space.

A major shift occurred when entities assisting consumers in the navigation of this vast new universe of content – primarily search firms – realized that advertisers were willing to pay more for ads that were actually clicked on by customers. This in turn resulted in an arms race among firms trying to develop algorithms and other approaches that could place online ads that were relevant to users.³⁶ This necessitated the development of platforms that could attract users and goad them into sharing more information about themselves – directly (*e.g.*, by filling out a form or buying a product), indirectly (*e.g.*, by typing in search terms), and surreptitiously (*e.g.*, by tracking users with cookies). (The success of this business model – *i.e.*, of monetizing consumer data – coupled with an increase in consumers’ interest in using the web to enhance real-world relationships, facilitated the rise of social media, a space currently dominated by Facebook.)

Google spearheaded this shift in Internet economics. While it was not the first firm to develop an effective algorithm for sorting search results or enter the online advertising business, it produced an incredibly effective integrated system for doing both.³⁷ Ever since, a growing number of companies throughout the ecosystem have eagerly sought to compete for a slice of the online advertising market, which has grown from an industry that generated \$9.6 billion in revenues in 2004 (the year of Google’s IPO) to one that neared \$90 billion in revenues in 2017.³⁸ The dominant format for digital ads is now

³⁴ See, *e.g.*, JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* 29 (2008) (“Consumer accessibility to Internet-enabled applications, coupled with the development of graphic-friendly World Wide Web protocols and the PC browsers to support them...marked the beginning of the end of proprietary information services [i.e., walled gardens].”).

³⁵ *Id.*

³⁶ See, *e.g.*, JOHN BATTELLE, *THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE* (2006) (providing a detailed overview of how this aspect of the online market evolved in the late 1990s and early 2000s).

³⁷ *Id.* See also Greg Lastowka, *Google’s Law*, 73 *Brook. L. Rev.* 1327, 1335-1351 (2008) (discussing the development of these components of Google’s business model).

³⁸ See *IAB Internet Advertising Revenues Report: 2017 Full Year Results*, at p. 2, Interactive Advertising Bureau (May 2018), https://www.iab.com/wp-content/uploads/2018/05/IAB-2017-Full-Year-Internet-Advertising-Revenue-Report.REV_.pdf (“2017 IAB Report”).

mobile, revenue from which has grown at a compound annual rate of 71.4% since 2012.³⁹ Google and Facebook dominate this space, having acquired some 60% market share.⁴⁰ Search ads remain a popular format, but revenue growth in that segment has slowed a bit in recent years.⁴¹ That said, it remains lucrative as it still comprises 44% of the overall digital ad market.⁴² Google dominates the search market – “more than 90% of all [I]nternet searches are taking place through” Google and its subsidiaries like YouTube⁴³ – and extracts a tremendous amount of revenue from it.

These structural shifts in the economics underlying many Internet businesses have had profound negative impacts on personal privacy. In particular, they have created a self-reinforcing cycle of data generation and collection on the one hand and the provision and consumption of targeted services on the other. Consumers, although generally aware of the privacy risks implicated by this general dynamic and wary of certain types of intrusive practices, continue to consume these services and provide, knowingly or not, the increasingly granular data that is necessary to keep these firms afloat. The result is a race among content firms to create new ways for collecting ever-more detailed information and using that data to micro-target ads and other online offerings.

To be sure, the lure of monetizing online data is not confined to search firms like Google or social media entities like Facebook. Tech titans – like Amazon, Apple, and Netflix – and other firms engage in similar practices. Although these companies dominate online advertising, there has been increased experimentation in recent years by a broad array of firms interested in entering this space and positioning themselves as the primary – or exclusive – mediator of the online experience and thus the sole harvester of the personal data that is generated. Consequently, there are few places in today’s society where some entity is not trying to extract data from consumers:

- Any computing device linked to the Internet – a laptop used at home; a desktop used at work; a smartphone used on the go – generates data that can be collected by a range of firms, including an operating system (e.g., Apple iOS or Android); web browser (e.g., Google Chrome); search engine (e.g., Bing); data broker (e.g., Acxiom); and content provider (e.g., YouTube).

³⁹ *Id.* at 9.

⁴⁰ See Rani Molla, *Google’s and Facebook’s share of the U.S. ad market could decline for the first time, thanks to Amazon and Snapchat*, March 18, 2018, Recode, <https://www.recode.net/2018/3/19/17139184/google-facebooks-share-digital-advertising-ad-market-could-decline-amazon-snapchat>.

⁴¹ 2017 IAB Report.

⁴² *Id.*

⁴³ See Jeff Desjardins, *How Google Retains More than 90% of Market Share*, April 23, 2018, Business Insider, <https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4>.

- A range of new smart home products leverage sensors and other communications technologies to generate vast amounts of data that assist in optimizing particular services and that provide more granular insights into individual and aggregate consumer behavior.⁴⁴
- Ad-supported Wi-Fi networks that blanket large areas in cities across the country rely on the data collected from users and passersby to demonstrate value to firms wishing to precisely target ads.⁴⁵ Billboards are increasingly leveraging similar kinds of data and collection techniques to ensure that ads are relevant.⁴⁶ And in addition to tracking online purchases, many large retailers also track in-store shopping, browsing, and buying habits of customers by using facial recognition and tapping into data emanating from their smartphones.⁴⁷
- In-home devices like smart TVs and voice assistants (e.g., Amazon’s Alexa) actively listen to consumers, gather relevant information, and respond to commands to purchase new products, change the channel, or search for the answer to a question. Similarly, wearable products like smart watches offer real-time portals into personal health data and other metrics that, in turn, help companies develop detailed portraits of users.⁴⁸
- The continued improvement of artificial intelligence, the foundation upon which many of these new “smart” products is built, relies on a constant

⁴⁴ See Kashmir Hill and Surya Mattu, *The House that Spied on Me*, Feb. 7, 2018, Gizmodo, <https://gizmodo.com/the-house-that-spied-on-me-1822429852>.

⁴⁵ See, e.g., Benjamin Dean, *The Heavy Price We Pay for ‘Free’ Wi-Fi*, Jan. 25, 2016, The Conversation, <https://theconversation.com/the-heavy-price-we-pay-for-free-wi-fi-52412> (articulating an array of concerns regarding the quid pro quo involved in providing “free” online services in exchange for the collection of granular personal information).

⁴⁶ See, e.g., Grant Gross, *Billboards Can Track Your Location, and Privacy Advocates Don’t Like it*, March 3, 2016, CSO, <http://www.csoonline.com/article/3040607/security/billboards-can-track-your-location-and-privacy-advocates-dont-like-it.html>; Marianna Kantor, *How Billboards are Challenging Digital Advertising*, June 13, 2018, ESRI, <https://www.esri.com/about/newsroom/publications/wherenext/out-of-home-advertising-and-location-intelligence/>.

⁴⁷ See, e.g., Erin Griffith, *Consumers Hate In-Store Tracking (But Retailers, Startups and Investors Love it)*, March 24, 2014, Fortune, <http://fortune.com/2014/03/24/consumers-hate-in-store-tracking-but-retailers-startups-and-investors-love-it/>; Annie Lin, *Facial recognition is tracking customers as they shop in stores, tech company says*, Nov. 23, 2017, CNBC, <https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html>.

⁴⁸ See, e.g., Olga Kharif, *Coming Soon to Your Smartwatch: Ads Targeting Captive Eyeballs*, May 12, 2015, Bloomberg, <http://www.bloomberg.com/news/articles/2015-05-12/coming-soon-to-your-smartwatch-ads-targeting-captive-eyeballs>.

stream of data in order to improve the underlying algorithms and make them more useful and responsive to consumers.⁴⁹

The ability to generate new data flows regarding a consumer's online and offline uses has intensified the rivalry among online firms that depend on digital advertising revenues. Because these new bits of information tend to be diffused across a number of disparate devices, networks, applications, and locations, these firms are focused on building platforms that can span these various uses and tie the data together more cohesively. In many ways, this presages a new era of "walled gardens," where online firms seek to serve as the exclusive portal through which users navigate nearly all online services. The business practices surrounding the creation of such "gardens" and the ways in which companies direct their users into them could foster anticompetitive behavior and thus bears monitoring by the Commission.

Some argue that ISPs are in prime position to collect data and engage in activities that undermine online privacy. This is not the case. Within the world of data collection and monetization, ISPs play a very small role. Because consumers' online activities increasingly span multiple devices and locations, it is nearly impossible for a single ISP to glean as much information about a particular user's online behavior as, say, Google.⁵⁰ In addition, more and more data that flows over broadband networks is encrypted, a dynamic that greatly limits the visibility an ISP might have into a customer's usage data.⁵¹ Moreover, even though some ISPs use customer data to develop and market ancillary services, the financial growth of these companies remains tied to subscription fees for core services, not digital ad revenue.

Understanding this basic dichotomy – between the incentives underlying the business models of content firms like Google on the one hand and other players, like ISPs, on the other – is essential to appreciating the fundamental nature of the digital ecosystem. It is also central to the new power dynamics evident in this space.

3. The FTC Must Recognize & Operationalize the Foundational Fact that Market Power in the Digital Ecosystem Revolves Around Data

At a very basic level, the antitrust laws, for which the FTC plays a key enforcement role, are concerned with power, specifically market power. Dominating a market allows a firm or group of firms to engage in activities that harm consumers. That harm has long been measured in terms of higher prices. The rise of the Internet economy, which revolves

⁴⁹ See, e.g., Brian Feldman, *The Future of Tech is Artificial Intelligence and That's Just Fine for Google*, May 18, 2016, New York Magazine, <http://nymag.com/selectall/2016/05/googles-back.html>.

⁵⁰ See, e.g., Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less Than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech (Feb. 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

⁵¹ *Id.*

around providing “free” products in exchange for consumer data, presents antitrust officials with a profound problem: in a market where most things are “free” and where competing services are a “click away,” are antitrust violations possible?⁵² Put another way: can consumers be harmed in a world where they are theoretically benefiting from a surfeit of choice for free products?

The common-sense answer to these questions is a resounding “yes, of course consumers can be harmed.” The endless spate of privacy violations, data intrusions, and “creepy” business practices of online firms provides significant evidence in support of this answer. Unfortunately, this foundational fact has not been operationalized in the prevailing frameworks that have shaped antitrust enforcement and consumer protection efforts at the FTC and elsewhere over the last few decades. That the FTC is convening hearings and seeking comment on precisely these issues demonstrates that the Commission recognizes this inadequacy and is interested in identifying new frameworks to guide its efforts going forward.

As a starting point, the FTC should explore the extent to which market power in the digital ecosystem revolves around the ability of firms to collect and monetize personal data. When viewed through this lens, it becomes clear that online firms wield considerable power.

This power manifests itself in the ability of content companies to shape the online experience for both good and ill. This stems from their having established themselves as essential to user enjoyment of the Internet.⁵³ And increasingly, their power extends

⁵² The literature on this issue is vast and continues to grow. Relevant examples include Frank Pasquale, *Paradoxes of Digital Antitrust: Why the FTC Failed to Explain its Inaction on Search Bias*, Harvard Journal of Law & Technology Occasional Paper Series (July 2013), <https://jolt.law.harvard.edu/assets/misc/Pasquale.pdf>; Lina M. Khan, *Amazon’s Antitrust Paradox*, 126 Yale L. J. 710 (2017), https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyeh.pdf. Cf. Elyse Dorsey, Jan M. Rybnicek & Joshua D. Wright, *Hipster Antitrust Meets Public Choice Economics: The Consumer Welfare Standard, Rule of Law, and Rent Seeking*, CP Antitrust Chronicle (April 2018), <https://www.competitionpolicyinternational.com/wp-content/uploads/2018/04/CPI-Dorsey-Rybnicek-Wright.pdf>.

⁵³ Some have gone so far as to label entities like Google and Facebook as public utilities. See, e.g., danah boyd, *Facebook is a Utility; Utilities Get Regulated*, May 15, 2010, Zephoria.org, <http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html> (“Your gut reaction might be to tell me that Facebook is not a utility. You’re wrong. People’s language reflects that people are depending on Facebook just like they depended on the Internet a decade ago. Facebook may not be at the scale of the Internet (or the Internet at the scale of electricity), but that doesn’t mean that it’s not angling to be a utility or quickly becoming one.”); Harry McCracken, *Of Course Facebook is a Utility!*, Nov. 17, 2013, Time.com, <http://techland.time.com/2013/11/17/of-course-facebook-is-a-utility/> (“On the web, the single biggest reason why giants collapse is because they don’t react quickly enough to indirect, emerging threats of this sort. If Facebook blithely dismissed them, it would be cause for alarm. But if the company is looking like a utility for the masses rather than a hot property for young people, it’s not a sign that the game has changed – it’s Facebook being what it’s been trying to be all along. And have you noticed? Utilities can be solid businesses. Maybe even better businesses than ones beloved by trendy

offline as well. Indeed, a true measure of a digital entity's power ought to be the extent to which it can shape outcomes in both the online world and the real world. To that end, the likes of Google, Facebook, and Amazon have the power to undermine rivals by prioritizing their own products in search results.⁵⁴ They can impact elections and shape public opinion by how they present the news.⁵⁵ They can decimate the workforce by pursuing automation as a growth strategy.⁵⁶ And they are increasingly serving as censors, moderating speech according to an ill-defined set of rules and norms.⁵⁷

Deciding whether or not to wield the power to meddle in the lives of users boils down to incentives. The difference in business models makes this clear. As previously noted, ISPs derive the lion's share of their revenues from residential and business subscriptions to voice, video, and/or data products. Content firms, on the other hand, are fueled by economic incentives that drive them to mine user data stemming from their use of a range of online and offline-but-still-connected services.⁵⁸ Accordingly, online firms like Facebook and Google have incentives to dominate – nay, monopolize – our online

teens.”); Jonathan Taplin, *Is it Time to Break up Google?*, April 22, 2017, N.Y. Times, <https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html> (arguing that Google “has all of the characteristics of a public utility” and observing that “We are going to have to decide fairly soon whether Google, Facebook, and Amazon are the kinds of natural monopolies that need to be regulated...”).

⁵⁴ See, e.g., Mark Scott, *Google Fined Record \$2.7 Billion in E.U. Antitrust Ruling*, June 27, 2017, N.Y. Times, <https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html> (reporting on a ruling by regulators in Europe that found that Google “unfairly favor[ed] some of its own services over those of rivals.”).

⁵⁵ See, e.g., Olivia Solon, *Facebook's Failure: Did Fake News and Polarized Politics Get Trump Elected?*, Nov. 10, 2016, The Guardian, <https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-election-conspiracy-theories> (reporting on the prominence of Facebook in the delivery and consumption of news by users and noting that “pressure is growing on Facebook to not only tackle the problem [of fake news] but also to find ways to encourage healthier discourse between people with different political views.”); Nicholas Thompson, *Facebook Opens Up About False News*, May 23, 2018, Wired, <https://www.wired.com/story/exclusive-facebook-opens-up-about-false-news/>.

⁵⁶ See, e.g., Danielle Paquette, *People are Worried Amazon will Replace Whole Foods Workers with Robots*, June 16, 2017, Wash. Post Wonkblog, https://www.washingtonpost.com/news/wonk/wp/2017/06/16/people-are-worried-amazon-will-replace-whole-foods-workers-with-robots/?utm_term=.461doc7b2coo; Spencer Soper, *Amazon Began Automating Warehouses A While Ago. Now its Machines Get Desk Jobs Too*, June 13, 2018, L.A. Times, <http://www.latimes.com/business/la-fi-amazon-automation-jobs-20180613-story.html>.

⁵⁷ See Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harvard L. Rev. 1598 (2018), https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf.

⁵⁸ See, e.g., *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Comments of the ACLP, FCC WC Docket No. 16-106 (submitted May 27, 2016), <http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/ACLP-Privacy-Comments-WC-Docket-No-16-106-052716.pdf> (discussing these incentives at length) (“ACLP Privacy Comments”).

experience because their bottom lines hinge on their ability to monetize data.⁵⁹ As such, they seek to entice consumers to use more of their services – *e.g.*, by giving them away for “free” – while surreptitiously hoovering up more and more data.⁶⁰ This also drives efforts to blunt meaningful enforcement of privacy and antitrust laws and to shift the focus – and blame – for online harms, real or theoretical, to others, most prominently the ISPs.⁶¹

Understanding the central role that data – and the desire to dominate data – plays in the business models of online firms will help to reorient the FTC’s thinking vis-à-vis market power in the digital ecosystem.

4. The FTC Should Make Clear that Enhanced Transparency is Essential to Bolstering Consumer Welfare in the Digital Ecosystem

Interactions between consumers and online firms revolve primarily around the harvesting of customer data. Indeed, as noted previously, the business model of most online firms depends not just on the ability to interact unimpeded with customers – it also relies on their ability to mine more and more granular information from users and monetize it by placing targeted ads. Although consumers place a relatively high value on their ability to receive free services in exchange for targeted ads,⁶² it is increasingly likely that, without government intervention – in the form of federal legislation, enhanced FTC oversight, etc. – online firms will be free to engage in ever more intrusive data collection practices. Accordingly, the Commission must explore the extent to which it can articulate and enforce transparency and disclosure standards in an effort to empower consumers with more insight into how their online data is being used. Without such action, the tactics of those battling for data supremacy will become even more opaque.⁶³

⁵⁹ For example, the vast majority – about 84% – of the revenues for Alphabet, Google’s parent company, stem from ad revenues, while just about all of Facebook’s revenues come from ads. These and other companies of their ilk sell and place ads based on their ability to more precisely target them, which stems from their intimate knowledge of consumers’ online behavior. See Jillian D’onfro, *Here are all the businesses owned by Google’s parent company and how they contribute to revenue*, Feb. 2, 2018, CNBC, <https://www.cnbc.com/2018/02/02/alphabet-business-units-revenue-contribution-and-ceos.html>; Emil Protalinski, *Over 90% of Facebook’s Advertising Revenue Now Comes from Mobile*, April 25, 2018, Venture Beat, <https://venturebeat.com/2018/04/25/over-90-of-facebooks-advertising-revenue-now-comes-from-mobile/>.

⁶⁰ See generally *ACLP Privacy Comments*

⁶¹ *Id.*

⁶² See, *e.g.*, Press Release, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, May 11, 2016, PR Newswire, <http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html> (reporting on the findings of a recent consumer poll regarding how much consumers value their ability to access free online services).

⁶³ See, *e.g.*, FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015) (describing many data gathering practices as occurring in black boxes that are designed to avoid close scrutiny).

The rise of artificially intelligent algorithms that can adapt in real-time as new information is fed in, the emergence of a universally connected “Internet of things,” and an overall explosion of digital data all raise by orders of magnitude the amount of information that is likely to be collected by edge providers. As consumers become more aware of intrusive data collection techniques, they are beginning to care more about the lengths to which a company is tracking them – *i.e.*, whether they consider those methods to be truly “creepy”⁶⁴ – and the ways in which a company encourages them to engage in socially unacceptable behavior so they can harvest more information.⁶⁵

Unfortunately, the relative laxity with which big tech firms are regulated in the online privacy context creates incentives for them to be even more clandestine with respect to their data collection methods. Waiting for harms to occur in this “black box society” and in a world where consumers aren’t aware of the full extent to which an online firm gathers and uses their data risks a race to the bottom in terms of further privacy intrusions that are overlooked or dismissed by regulators as “business as usual.”

5. The FTC Must Stake Out a Lead Role in Enforcement

Numerous limitations impede more robust FTC action in a range of contexts.⁶⁶ Ultimately, Congressional action is needed to empower the Commission with enhanced authority and a greater variety of tools with which to police the digital ecosystem. Until that occurs, the Commission can and should act to maximize the authority it already possesses in an effort to stake out a lead role in addressing the myriad of competition issues and consumer harms emerging in this space. There is much that can be done. For example, the FTC could seek to:

- Expedite reviews of alleged harms to evince a more real-time and responsive posture. Fast-tracking inquiries of especially pernicious behavior, like the ongoing investigation of Facebook’s actions vis-à-vis Cambridge Analytica, should become the norm.
- Impose maximum fines to punish misdeeds.

⁶⁴ See Omer Tene and Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale J. L. & Tech. (2013) (observing that “...intuitions and perceptions of how our social values should align with our technological capabilities are highly subjective. And, as new technologies strain our social norms, a shared understanding of that alignment is even more difficult to capture. The word “creepy” has become something of a term of art in privacy policy to denote situations where the two do not line up.” *Id.* at 60).

⁶⁵ The consumer pushback against a device like Google Glass is instructive. For an overview, see Jake Swearingen, *How the Camera Doomed Google Glass*, Jan. 12, 2015, The Atlantic, <http://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/>.

⁶⁶ See, e.g., *Statement of the FTC* at p. 6.

- Bolster the review of transactions involving edge/tech companies by, among other things, exploring the impact of the merger on the new entity's ability to collect and monetize data.

The FTC can also begin harmonizing state UDAP enforcement – and state action on issues like privacy generally. The goal should be to create and maintain as comprehensive a safety net for consumer privacy as possible. In particular, the Commission could:

- Convene a working group that brings together state AGs and other experts to develop a model framework for balancing federal and state enforcement in key areas.
- Coordinate oversight and enforcement with state counterparts as appropriate.
- Issue guidance – *e.g.*, via letters, filings, comments, etc. – to state and local officials exploring privacy and data security rules.