The Honorable David Cicilline, Chair
The Honorable F. James Sensenbrenner, Ranking Member
House Committee on the Judiciary
Subcommittee on Antitrust, Commercial, and Administrative Law
2138 Rayburn House Office Building
Washington, DC 20515

Statement for the Hearing on Online Platforms and Market Power
Part 3: The Role of Data and Privacy in Competition

Friday, October 18, 2019

Dear Chairman Cicilline and Ranking Member Sensenbrenner:

Thank you for hosting this hearing and for inviting my thoughts on this topic. This statement reflects my position as a legal scholar examining the intersection of competition and technology, as well as my experience as an entrepreneur and executive in the digital advertising industry since 2007.

In my twelve years working in and researching digital advertising, I have closely watched the rise of modern high-tech industries that now drive our economy. I have observed the markets for online search, social networking, instant messaging and advertising software transition from being fiercely contested by many upstart firms to intensely consolidated by a handful of tech giants, and I have written about how this consolidation has affected consumers and the dynamism of the American economy.

What I have learned is that, when it comes to our data, the degree of consumer privacy is closely linked with the degree of competition in the marketplace. Many of the high-tech services that Americans use every day may technically be "free", but market consolidation allows companies like Alphabet (the parent company of Google) and Facebook to harm consumers not by escalating prices, but rather, by diminishing quality by eroding privacy terms. This is why I have argued that regulators need to rethink their approach by considering the issue of privacy as part of the question of quality—which, along with price, is the other crucial factor when considering antitrust enforcement.[1]

[1] Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 Berkeley Bus. L.J. 39 (2019).

The online advertising market has an insatiable demand for consumer data. As Google and Facebook increasingly ignore user privacy, they collect an ever-growing amount of data from their users' emails, search queries, browsers, social network likes, and online video consumption, to target consumers and dominate online advertising. The two firms are now a duopoly that control approximately 60% of the total U.S. internet advertising market, as well as the vast majority of year-over-year growth within it.[2] Google and Facebook do not simply sell advertisements to marketers that appear on their own properties. They also control the advertising software and real-time exchanges that online publishers go through to sell their own advertising inventory.

While there is not space in this statement to holistically address all the problems related to data, privacy, and competition, in my remarks below, I focus on the following overlooked issues:

1. The erosion of privacy for users of Facebook and Google over time
2. Restrictions around data portability help firms maintain and grow their market power
3. The inability to opt-out of online tracking renders competitors' privacy-focused strategies obsolete
4. Overly complicated terms of service prevent consumers from making informed decisions
5. Increased collection of user data allows firms to exploit consumers
6. A more competitive landscape may compel firms to pay users for their data

1. The erosion of privacy for users of Facebook and Google over time

Facebook's evolution provides a telling example of how, when competition is eliminated, quality erodes. When Facebook launched in 2005 it faced fierce competition from rival social networks like MySpace, Orkut, Bebo, and Friendster. To differentiate itself, Facebook adopted the position of the social network that cared about user privacy. "We do not and will not use cookies to collect private information from any user," declared its privacy policy at the time.[3] However, as the number of competitors decreased, Facebook began tracking users on an additional 8 million-plus other sites and mobile apps—anything that embeds Facebook's Like button or plugs into

[2] Sheila Dang, *Google, Facebook Have Tight Grip on Growing U.S. Online Ad Market: Report*, Reuters (June 5, 2019), https://www.reuters.com/article/us-alphabet-facebook-advertising/google-facebook-have-tight-grip-on-growing-u-s-online-ad-market-report-idUSKCN1T61IV.

[3] *Facebook Privacy Policy*, FACEBOOK.COM (Dec. 30, 2004), http://www.thefacebook.com/policy.php [https://web.archive.org/web/20050107221705/http://www.thefacebook.com/policy.php].

Facebook's software—to sell ads. It gets away with this because users who might want to leave the social network no longer have any other choice.

The story of Google's rise to dominance tells a parallel story. When Google acquired the advertising software company DoubleClick in 2007, privacy advocates were concerned that the new Google would leverage its dominance to decrease consumers' privacy. Specifically, they were concerned Google would combine its ability to identify consumers online (through Gmail, for example), with DoubleClick's ability to extensively track users anonymously, in order to know exactly what specific, real people do online. In spite of this concern, the Federal Trade Commission approved the merger, dismissing the likelihood that less competition would trigger consumer privacy problems. Yet in 2016, after Google had further entrenched its dominance in the search market, the ad server software market, and the advertising exchange software market, Google deprecated consumer privacy in precisely the way some experts forecasted but the FTC dismissed.[4]

2. **Restrictions around data portability help firms maintain and grow their market power**

There is another important way that companies can use data to interfere with competition and hurt consumers in the process—and that is, by interfering with data portability. Google search data can be easily accessed in Google's analytics software alone. Data in Google's analytics software can be easily ported into Google advertising software, but not the advertising software of competing firms. This type of behavior allows a company to leverage a dominant position in one market into a dominant one in another. Free markets work when firms purchase a product because of its merits, not simply because it is tied to another product they have no choice but to buy.

3. **The inability to opt-out of online tracking renders competitors' privacy-focused strategies obsolete**

Companies' policies around online tracking can make it difficult for other firms to compete by offering services with higher levels of privacy. When Snapchat (Facebook's largest social network competitor) entered the market, it promised users it would not track them across the web as a way to differentiate itself. In an ideal marketplace, that means consumers who do not like Facebook's practice of tracking them online could opt out of Facebook and choose to use Snapchat instead. But there is just one problem: Facebook continues to track users even after they deactivate or delete their accounts. Since users cannot escape Facebook's privacy intrusions by choosing a different service, there is less incentive to switch to a new service, which makes it

[4] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, ProPublica (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.

difficult for competitors to compete on privacy.

4. Overly complicated terms of service prevent consumers from making informed decisions

Competition is undermined when companies bury their privacy and data policies in long terms and conditions agreements that consumers cannot read or simply do not understand—Google's Terms of Service agreement that deals with privacy is 27 pages long.[5] When a user signs up for Google's email service, Google clearly states that Gmail is "free." However, in reality, the service comes at the cost of consumers' personal data being collected and used for multiple purposes, including personalized ads. Google buries this information in a long Terms of Service agreement, just as credit card companies once buried interest rates in long incomprehensible financial contracts. Today, nuances in privacy terms are relegated to investigative journalists to discover and explain. When the media does report on them—as they did around Google's practice of letting employees and contractors read Gmail users' emails[6]—consumers often switch to a competitor that offers a better product or service.

5. Increased collection of user data allows firms to exploit consumers

When companies hold large troves of consumer data, they control more data that can be stolen or used in predatory ways, such as using data to target and manipulate vulnerable individuals for political, social or commercial means. For example, earlier this year, we observed a company using what it knows about people to suppress housing ads to people based on their race, religion, or national origin.[7]

6. A more competitive landscape may compel firms to pay users for their data

In online advertising markets, if competition worked as it should, companies might pay users for the right to gather information about them and show them targeted ads. The advertising companies that extract data from consumers make billions of dollars selling behaviorally targeted advertising. Online ads are traded in real-time advertising exchanges, similar to stock exchanges, and consumers' data is part of this process. According to a recent study released by Google, the value of the ads that Google sells drops by 52% on average, when Google cannot use consumers'

---

[5] Gmail Terms of Use: Terms and Privacy, https://www.google.com/mail/help/terms_of_use.html (last visited Sept. 9, 2019); Google, Google Privacy Policy (Jan. 22, 2019), https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en.pdf.

[6] Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*, Wall St. J. (July 2, 2018), https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442.

[7] Katie Benner, Glenn Thrush & Mike Isaac, *Facebook Engages in Housing Discrimination with Its Ad Practices, U.S. Says*, N.Y. Times (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html.

data to target them.[8] It is technically feasible to compensate consumers for the ability to collect information about them in order to show them more targeted ads—as evidenced by at least one browser company doing so today.

Historically, it has been the role of the federal government to actively intervene in emerging product markets—including foods, drugs, cars, and financial products—to ensure that free markets work for consumers. This is especially true when products are dangerous, have hidden or deferred risk, or depend on consumers assenting to long terms they cannot read or understand. Our government should pass legislation that protects consumers from companies' exploitative data practices and also grants them the ability to opt-out of behaviorally targeted advertising. Our antitrust laws can also help solve problems related to data and privacy. Here, for example, enforcers can recognize the consumer harm in the erosion of quality and privacy, and how friction around data portability helps firms maintain and leverage their market power. The issues around technology, data, and privacy are complicated, but solving them is less tricky that many companies would have Congress believe.

Thank you and I would be happy to answer any questions that the committee may have.

Respectfully,

Dina Srinivasan

[8] Deepak Ravichandran & Nitish Korula, Effect of Disabling Third-Party Cookies on Publisher Revenue, Google (Aug. 27, 2019), https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf.