



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

3. The identification and measurement of market power and entry barriers, and the evaluation of collusive, exclusionary, or predatory conduct or conduct that violates the consumer protection statutes enforced by the FTC, in markets featuring “platform” businesses.

Antitrust

For Consumers Union’s¹ comments on antitrust and competition issues pertaining to this topic please see: *Comments of Consumers Union—Antitrust and Competition Issues*.

Consumer Protection

The emergence of giant, cross-service internet platforms such as Facebook, Google, and Twitter, present at least two novel consumer protection issues that the Federal Trade Commission (FTC) should address. First, platforms that offer disparate (and often not consumer-facing) services has led to increased *out-of-context data collection*: that is, collection and correlation of extensive consumer data profiles in surprising—and potentially objectionable—ways. Some of this is relatively transparent, though consumers may still object to the consolidation of data sets from different services. For example, over time Google has broken down its silos from its different products to create a more unified Google service as opposed to separate Gmail, Search, and

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.

YouTube products. Google offers some tools to keep these experiences separate, though users may not be aware of them, and when they do, they may be difficult to use. For example, Google offers a “Location History” control to limit Android’s passive collection of persistent geolocation data; however, this control has no effect on geolocation data collected and associated with other products such as Search, Maps, and Weather.² This aggregation of data across services has become especially pervasive given extensive merger and acquisition activity in the technology sector. Some companies have sought to forestall concerns by making promises not to combine and use data across different products. For example, in the wake of its acquisition by Facebook, WhatsApp promised users that nothing would change from its policy of not using mobile phone numbers for advertising.³ Nevertheless, in 2016, Facebook announced that it would begin using WhatsApp phone numbers for friend suggestions and ad targeting on Facebook.⁴ Despite complaints from advocates, the FTC to date has taken no action.⁵

Still more concerning is the less visible—and more extensive—data collection enabled by platforms acting as a service provider for other companies. For example, both Google and Facebook provide advertising, analytics, and social widgets to a massive number of other publishers’ websites and applications. Various studies have shown that Facebook and Google track users on a tremendous number of third-party sites;⁶ one survey from the FTC’s Office of Technology Research and Investigation found that Google and Facebook were embedded on 87.5 percent and 69 percent of major websites.⁷ Industry defenders used to call cross-site behavioral data collection “anonymous,” meaning the data was not easily tied to real-name identity. That fact was relied upon by the FTC in closing its investigation into the DoubleClick acquisition of the data broker Abacus in 2002: the Commission declined to take action in part because “it appears that DoubleClick did not combine PII from Abacus Direct with clickstream data from client websites.”⁸

² Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), <https://apnews.com/828aefab64d4411bac257a07c1af0ecb>.

Facebook also collects geolocation in the background when consumers are not using the application. Janelle Nanos, *Every Step You Take*, BOSTON GLOBE (July 2018), <https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/>.

³ *Facebook*, WHATSAPP BLOG (Feb. 19, 2014), <https://blog.whatsapp.com/499/Facebook>; *Letter to Erin Egan, Facebook, and Anne Hoge, WhatsApp*, FED. TRADE COMM’N (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

⁴ *Looking Ahead for WhatsApp*, WHATSAPP BLOG (Aug. 25, 2016), <https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp>.

⁵ *WhatsApp Complaint*, ELEC. PRIVACY INFO. CTR. (Aug. 29, 2016), <https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf>.

⁶ *E.g.*, Stephen Englehardt & Arvind Narayanan, *Online Tracking, A 1-Million-Site Measurement and Analysis*, OPENWPM (2016), http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Ibrahim Altaweel *et al.*, *Web Privacy Census*, J. OF TECH. SCI. (2015), <https://techscience.org/a/2015121502/>.

⁷ Justin Brookman, *et al.*, *Cross-Device Tracking: Measurement and Disclosures*, 2 PROCEEDINGS ON PRIVACY ENHANCING TECH. 133-48 (2017), <https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf>. Indeed, these numbers may be low as they do not account for server-to-server communications that are undetectable to end users.

⁸ *Letter to Christine Varney, Re: DoubleClick, Inc.*, FED. TRADE COMM’N (Jan. 22, 2001), https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.

The separation between offline identity and behavioral data has fallen by the wayside in recent years: now both Google and Facebook (as well as others who have access to identity data) collect cross-site and -app data across multiple user devices tied to a user identity. This practice is not widely appreciated by consumers⁹ and was the subject of bipartisan opprobrium during the recent Facebook-Cambridge Analytica hearings in the Senate and House of Representatives.¹⁰

In response, the Federal Trade Commission should:

- Encourage companies to be more transparent about actual data practices in privacy disclosures—instead of just vaguely asserting broad rights to collect and use data in a privacy policy. As discussed in more detail in response to Topic 1,¹¹ the Commission’s guidance should recognize that privacy policies are not useful means of conveying information directly to consumers, but they can be studied and monitored by researchers, regulators, the press, and ratings services such as Consumer Reports. Detailed transparency is unlikely to be sufficient by itself to safeguard users’ privacy but can introduce information and accountability to the marketplace.
- Aggressively enforce against companies that fail to live up to their privacy representations or offer tools that do not work as described, and continue to use the FTC’s unfairness authority under Section 5 to pursue out-of-context data collection engaged in without permission. The FTC has brought many important actions against privacy violations, but the Commission should continue to press the boundaries of its limited privacy authority to sufficiently deter practices that frustrate user autonomy and decision-making.
- Request Congress to grant the FTC new statutory authority to issue rules around out-of-context data collection. The burden to safeguard personal information should not fall entirely on consumers—large platforms today offer myriad settings with some degree of control, but they are difficult to manage, offer incomplete protections, and sometimes fail to work as advertised. New privacy law should dictate that data collection and sharing practices accord with reasonable expectations and preferences.

Another feature of large platforms that merits the FTC’s attention is the fact that they can be manipulated and misused on an unprecedented scale, including for consumer fraud. While

⁹ “But, as it has become apparent in the past year, we don’t really know who is seeing our data or how they’re using it. Even the people whose business it is to know don’t know. When it came out that the consulting firm Cambridge Analytica had harvested the personal information of more than fifty million Facebook users and offered it to clients, including the Trump campaign, the *Times*’ lead consumer-technology writer published a column titled “I Downloaded the Information That Facebook Has on Me. Yikes.” He was astonished at how much of his personal data Facebook had stored and the long list of companies it had been sold to. Somehow, he had never thought to look into this before.” Louis Menand, *Why Do We Care So Much About Privacy?*, THE NEW YORKER (June 18, 2018), <https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy>.

¹⁰ Natasha Singer, *What You Don’t Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

¹¹ For more on this issue, please see Consumers Union response to Topic 1: *The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings*.

traditional product and information markets were more manually curated, online platforms allow millions (and in some cases, billions) of consumers to interact with others as well as businesses (both well-meaning and less-so) with limited intervention and overhead. Facebook, for example, employs relatively few people for a company its size (its market cap is over \$500 billion, or approximately \$21 million for each of its 25,000 employees); and only a small percentage are dedicated to eliminating malfeasance on the platform. These platforms are largely insulated from legal responsibility to police their services by Section 230 of the Communications Decency Act, which gives companies broad immunity for how others use their services.

Clearly, there are substantial benefits to both consumers and businesses in engaging on these types of platforms. However, there is also evidence that malicious actors can pervert the way these platforms function without sufficient redress from the platform operators. The 2016 election is but the starkest example of how foreign powers can simulate grassroots opinion on social media to further their own ends. YouTube’s automated recommendation has been repeatedly gamed to promote vile and discredited conspiracy theories.¹² Vague promises that “artificial intelligence” may be able to address these problems at some point in the future are not entirely reassuring, as this technology is still potentially years away, not guaranteed to work, and may be compromised by the limitations and biases of the people who design it.¹³ However, there have been some signs in recent months that many of the platforms are taking some more proactive measures to reduce abuse on their services.¹⁴

While some of this behavior is obviously beyond the FTC’s purview, it is clear that platforms enable extensive commercial fraud and malicious anti-consumer behavior as well as political

¹² “The algorithm has been found to be promoting conspiracy theories about the Las Vegas mass shooting and incentivizing, through recommendations, a thriving subculture that targets children with disturbing content...Google has responded to these controversies in a process akin to Whac-A-Mole: expanding the army of human moderators, removing offensive YouTube videos identified by journalists and de-monetising the channels that create them. But none of those moves has diminished a growing concern that something has gone profoundly awry with the artificial intelligence powering YouTube.” Paul Lewis, *‘Fiction is Outperforming Reality’: How YouTube’s Algorithm Distorts Truth*, THE GUARDIAN (Feb. 2, 2018), <https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth>. Google recently announced a plan to combat this problem. Issie Lapowsky, *YouTube Debuts Plan to Promote and Fund ‘Authoritative’ News*, THE GUARDIAN (July 9, 2018), <https://www.wired.com/story/youtube-debuts-plan-to-promote-fund-authoritative-news/>.

¹³ Sarah Jeong, *AI is an Excuse for Facebook to Keep Messing Up*, THE VERGE (Apr. 13, 2018), <https://www.theverge.com/2018/4/13/17235042/facebook-mark-zuckerberg-ai-artificial-intelligence-excuse-congress-hearings>. For more on the limitations of algorithms and artificial intelligence, see our comments in response to Topic 9: *The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics*.

¹⁴ Anthony Ha, *Facebook will Allow You to See All the Active Ads from any Page*, TECHCRUNCH (June 28, 2018), <https://techcrunch.com/2018/06/28/facebook-ad-transparency/>; Craig Timberg & Elizabeth Dwoskin, *Twitter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk*, WASH. POST (July 6, 2018), https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.bd9bbe4cf1d1.

attacks. Shoppers on Amazon—which processes half of all online sales¹⁵—face a massive fraudulent review ecosystem designed to simulate and obscure truthful information about millions of products, which Amazon has thus far been unable or unwilling to control.¹⁶ Social media platforms are dogged by accounts promoting a wide variety of questionable products and services,¹⁷ promoted through fake followers and fake engagement designed to exploit algorithms that reward such behavior.¹⁸ Fraud in online programmatic advertising is estimated to approach 30% despite industry efforts to address it.¹⁹ In many of these cases, not enough industry actors have sufficient incentives, let alone legal obligations, to try to reduce the scope of illegal activity on their platforms (further, they are in sole possession of the most relevant metrics in assessing the extent of misbehavior). In some cases, the companies benefit directly from the bad behavior; in others, they are judged by analysts based on the scope of their engagement, and as such may be loath to root out all the simulated traffic that distorts the information conveyed through these services. Ultimately, many of the costs of this misbehavior are borne by consumers in the form of higher prices or degraded services.

The FTC can do a number of things to help address these problems.

- Regularly update guidance on what sort of emerging online behaviors violate Section 5 of the FTC Act. The Commission has published solid guidance on native advertising and paid endorsements, but many tactics (such as purchasing followers to artificially amplify signals that may lead to more traffic) are not explicitly covered. The FTC should appoint a task force to keep its guidance up to date.
- More aggressively enforce against companies that abuse platforms to artificially amplify traffic or otherwise deceive consumers. The FTC has brought a number of important cases but clearly has not sufficiently deterred platform abuse.
- Explore ways to incentivize platforms to more aggressively police their platforms for deceptive, unfair, or otherwise illegal behavior.
- Explore ways to foster diversity of content and reduce the risk of algorithmic gaming. Potential solutions could interoperability, independent third-party algorithmic sorting, or

¹⁵ Ingrid London, *Amazon's Share of the US e-Commerce Market is Now 49%, or 5% of All Retail Spend*, TECHCRUNCH (July 13, 2018), <https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/>.

¹⁶ Laura Stevens, *How Sellers Trick Amazon to Boost Sales*, WALL ST. J. (July 28, 2018), <https://www.wsj.com/articles/how-sellers-trick-amazon-to-boost-sales-1532750493>.

¹⁷ Annie Singer & Joanna Laznicka, *Fake and Deceptive Use of Instagram: How to Spot False Influencers*, <http://smartlinkup.com/fake-instagram-influencers/>.

¹⁸ Nicholas Confessore, *et al.*, *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), <https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html>; Michael H. Keller, *The Flourishing Business of Fake YouTube Views*, N.Y. TIMES (Aug. 11, 2018), <https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html>.

¹⁹ Alexandra Bruell, *Fraudulent Web Traffic Continues to Plague Advertisers, Other Businesses*, WALL ST. J. (Mar. 28, 2018), <https://www.wsj.com/articles/fraudulent-web-traffic-continues-to-plague-advertisers-other-businesses-1522234801>.

more robust options for users to access social media feeds in chronological order, unmediated by algorithms.

- Explore how reducing fraudulent online content and other misbehavior could be a beneficial result of protecting competition and innovation in platforms, and whether that benefit could be a relevant consideration in antitrust investigations involving platforms.

Respectfully submitted,

Justin Brookman
Director, Consumer Privacy
& Technology Policy

Consumers Union
1101 17th Street, NW
Suite 500
Washington, DC 20036