Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

Re: Petition for Rulemaking to Prohibit Surveillance Advertising

---

TABLE OF CONTENTS

PETITION FOR RULEMAKING

Accountable Tech hereby respectfully petitions the Federal Trade Commission ("FTC"), pursuant to the Administrative Procedure Act and the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 to initiate rulemaking to prohibit the anticompetitive practice of surveillance advertising.

INTEREST OF THE PETITIONER

Accountable Tech is a nonpartisan, nonprofit organization that advocates for structural reforms to repair our information ecosystem and foster a healthier and more equitable democracy.

I. INTRODUCTION

On July 9, 2021, the White House issued Executive Order 14036 (EO) aimed at empowering a constellation of federal agencies to combat monopolies and eliminate anticompetitive practices wielded by dominant digital platforms. As part of that effort, the EO encourages the Federal Trade Commission (FTC) to use its rulemaking authority to address certain "unfair data collection and surveillance practices" that harm competition, consumers, and society.[1] The surveillance practices employed by dominant platforms are central to their business models, and serve as the enabling mechanism for much of their anticompetitive conduct. As such, directly addressing the underlying incentive structure that drives these harms must be at the heart of any measure aimed at curbing them. To this end, the FTC should use its rulemaking authority to prohibit surveillance advertising as an unfair method of competition.

Over the past decade, surveillance advertising has become a highly lucrative business model dependent upon pervasive tracking and profiling for the purpose of selling hyper-

[1] Exec. Order No. 14036, 86 Fed. Reg. 15069 (July 14, 2021).

personalized ads.[2] Surveillance-based advertising is an inherently unfair method of competition which both relies upon, and cyclically reinforces, monopoly power. Because many digital markets are prone to "tipping"—whereby early competition is for the entirety of the market—dominant firms have gained access to massive user bases and self-perpetuating data advantages that provide high barriers to entry and easy leverage into adjacent markets.[3] On this foundation, surveillance advertising fuels a toxic feedback loop: dominant firms are uniquely situated and incentivized to (1) unfairly extract and monetize more user data; (2) unfairly integrate that data across business lines; and (3) actively suppress competition. As this flywheel accelerates, so too does the race to the bottom amongst rivals seeking to close ever-widening data gaps.

The rise of today's dominant surveillance advertising firms illustrates these dynamics. For example, Facebook and Google initially faced robust competition with other cost-free offerings. Each company built scale not just through high-quality products, but also high-minded promises that earned users' trust. However, after gaining control of those winner-take-all markets[4] and locking in users with high switching costs, both firms began to renege on those commitments. Each eroded privacy protections and leveraged their power to establish a ubiquitous network of touchpoints throughout the digital economy. Counter to what they promised consumers when they were first flourishing, the surveillance advertising giants grew lucrative empires by tracking users across their platforms and third-party entities, and building comprehensive data profiles in order to micro-target audiences with more and more invasive ads.

---

[2] Natasha Lomas, *International Coalition Joins the Call to Ban 'Surveillance Advertising*, Tech Crunch (June 23, 2021), https://techcrunch.com/2021/06/23/international-coalition-joins-the-call-to-ban-surveillance-advertising/.
[3] Majority Staff of H. Subcomm. On Antitrust, Comm. and Admin. L. of the H. Comm. on the Judiciary, 116th Cong., Investigation of Competition in Digital Markets at 42-45 (2020), https://fm.cnbc.com/applications/cnbc.com/resources/editorialfiles/2020/10/06/investigation_of_competition_in_digital_markets_majority_staff_report_and_recommendations.pdf.
[4] Supra note 3 at 37.

As a result, Facebook and Google now own roughly three-quarters of the nation's booming digital ad market. Even as that market has exploded from $9.6 billion in 2004 to $140 billion as of 2020, their duopoly has consistently increased its share of the pie and captured more than 80% of market growth in each of the last six years.[5] Underscoring the monumental barriers to entry, the only other company that has managed to become a significant player is Amazon—another dominant firm that has exploited its unique access to troves of consumer and business data across platforms to engage in surveillance advertising. The three digital giants now control roughly 90% of the online ad market and collect more than half of *all* ad dollars spent in the U.S.[6]

These dominant firms have used surveillance advertising to reinforce unfair advantages across business lines, stamp out meaningful competition throughout the digital economy, and broadly abuse their market power in ways that cause significant harm to businesses, consumers, and society. Companies like Facebook and Google—who compete with publishers for advertising—have exploited the superior targeting capacity derived from their wealth of user data and attention to cannibalize the digital ad market and siphon critical revenue away from publishers. Moreover, as the surveillance advertising firms have entrenched their dominance, they have compelled resource-starved publishers to effectively hand over proprietary audience data by embedding their tracking tools, further accelerating this consolidation of power.

Advertisers, too, suffer in myriad ways from the anticompetitive nature of surveillance advertising. As explained in greater detail below, the overwhelming majority of online display ads are now purchased through opaque, automated auctions hosted by dominant firms who have both

---

[5] Accountable Tech, *Facebook and Google's Consolidation of U.S. Digital Ad Market* (last accessed: September 22, 2021), https://www.accountabletech.org/wp-content/uploads/Facebook-and-Googles-Consolidation-of-US-Digital-Ad-Market.pdf.

[6] Keach Hagey and Suzanne Vranica, *How COVID-19 Supercharged the Advertising 'Triopoly' of Google, Facebook, and Amazon,* The Wall Street Journal (March 19, 2021), https://www.wsj.com/articles/how-covid-19-supercharged-the-advertising-triopoly-of-google-facebook-and-amazon-11616163738.

the ability and the incentive to rig the game. That's exactly what they've done. For example, Facebook has been caught repeatedly and knowingly inflating metrics, essentially defrauding advertisers for years,[7] while Google extracts a "monopoly tax on billions of daily transactions"[8] and engages in flagrant self-dealing.[9] The dominant surveillance advertising firms are only able to get away with such anticompetitive conduct because there is functionally no other avenue by which to reach much of the population with digital ads. The harms inflicted on publishers and advertisers are ultimately passed on to consumers, who find themselves living in local news deserts and paying higher prices for goods.

Consumers also suffer directly from surveillance advertising. For users of nominally "free" products, paid for in the form of personal data and attention, each new invasion of privacy and degradation of services is an effective price hike. In healthy markets, few consumers would tolerate the pervasive tracking, exploitation, and manipulation to which dominant firms currently subject them in service of their surveillance advertising businesses. This includes the evolution of influential platforms like Instagram and YouTube that now curate each user's experience and information sphere to maximize engagement, using exhaustive behavioral profiles and powerful prediction algorithms—built on the same infrastructure and incentives as their ad delivery tools—to keep people clicking, so they can wrest more data and serve more personalized ads. This is not how these platforms functioned when they were forced to compete on the merits to gain market

---

7 Natasha Lomas, *Facebook Knew for Years Ad Reach Estimates Were Based on 'Wrong Data' But Blocked Fixes Over Revenue Impact, Per Court Filing,* Tech Crunch (February 18, 2021), https://techcrunch.com/2021/02/18/facebook-knew-for-years-ad-reach-estimates-were-based-on-wrong-data-but-blocked-fixes-over-revenue-impact-per-court-filing/.

8 *Texas v. Google,* No. 4:20-CV-957-SDJ at 12 (E.D. Tex. December 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216%20COMPLAINT_REDACTED.pdf.

9 Laura Kayali, *Google Agrees to Advertising Changes After €220M French Antitrust Fine*, Politico (June 7, 2021), https://www.politico.eu/article/france-competition-google-advertising-antitrust-fine/.

share; it is only their monopoly power and ubiquity that lets them extract profits from users in increasingly ruthless ways without consequence.

These harms are an inevitable consequence of the business model. Surveillance advertising empowers dominant firms to unfairly extract, monetize, and integrate data from captive users. At scale, those firms can gather information on people well beyond what people willingly offer. The inescapable data dragnet equips surveillance advertising giants with a decisive advantage over rivals – an unearned subsidy that erects artificial barriers against companies that would outcompete them on a level playing field. These practices exacerbate lock-in, allowing dominant firms to leverage into other digital markets and manipulate users to capture more attention, and in turn, raise costs on publishers and advertisers. This effect continues in a self-perpetuating cycle that entrenches their power, and also forces smaller players to emulate their abuses to survive, sparking a race to the bottom amongst all market participants. As such, even though surveillance advertising openly degrades product quality, the competitive edge dominant firms gain by employing the business model easily outstrips any loss of market share they would otherwise experience.

These anticompetitive features are intractably interdependent and mutually reinforcing, setting into motion a spiral of market concentration and escalatory harms. Neither ex-post enforcement against individual abuses, nor efforts to disaggregate and narrowly address enumerated components of this business model, are sufficient to stop the flywheel from turning. In order to prevent further harm to American businesses and consumers, the Commission must use its rulemaking authority under Section 5 of the FTC Act to prohibit surveillance advertising as an unfair method of competition.

II. LEGAL BASIS FOR RULEMAKING UNDER "UNFAIR METHODS OF COMPETITION"

Though the FTC has typically exercised its "unfair methods of competition" (UMC) authority through enforcement actions, the Commission can also promulgate legislative rules under UMC in accordance with the Administrative Procedure Act.[10] Section 5 of the Federal Trade Commission Act (FTC Act) declares that "*[u]nfair methods of competition* in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[11] Section 6 grants the Commission the authority to "make rules and regulations for the purposes of carrying out the provisions of this subchapter."[12]

A pair of misperceptions have created unnecessary confusion about whether the FTC can issue rules under its UMC authority at all. First, the FTC has only ever deployed its antitrust rulemaking powers once, in 1967,[13] which some have misinterpreted as evidence the FTC lacks the power to promulgate UMC regulations. Dormant, however, is distinct from defunct. The fact that an agency like the FTC has infrequently exercised duly-delegated rulemaking powers has no bearing on whether it can do so in the future. Indeed, the D.C. Circuit held in 1973 that the FTC could issue substantive rules to effectuate the FTC Act's Section 5 proscriptions.[14] Recently the FTC has also acknowledged its ability to conduct competition rulemaking.[15]

---

[10] *See generally,* Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. Chic. L. Rev. 357 (2020); Justin (Gus) Hurwitz, Chevron *and the Limits of Administrative Antitrust*, 76 Univ. Pitt. L. Rev. 209 (2014); Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 Univ. Penn. J. Bus. L. 645 (2018).

[11] 15 U.S.C. § 45(a)(1) (emphasis added).

[12] 15 U.S.C. § 56(g).

[13] *Discriminatory Practices in Men's and Boys' Tailored Clothing Industry*, 16 C.F.R. Part 412 (1968); 32 Fed. Reg. 15584 (1967).

[14] *National Petroleum Refiners Association v. F.T.C.*, 482 F2d 672, 698 (D.C. Cir. 1973) ("We hold that under the terms of its governing statute, 15 U.S.C. § 41 et seq., and under Section 6(g), 15 U.S.C. § 46(g), in particular, the Federal Trade Commission is authorized to promulgate rules defining the meaning of the statutory standards of the illegality the Commission is empowered to prevent.").

[15] Federal Trade Commission, *FTC to Hold Workshop on Non-Compete Clauses Used in Employment Contracts* (Dec 5, 2019), ("Should the FTC consider using its rulemaking authority to address the potential harms of non-compete clauses, applying either UMC or UDAP principles?").

Second, over the years Congress has repeatedly curtailed elements of the Commission's Section 5 rulemaking authority, constraints which some mistakenly believe apply to UMC. As enacted in 1914, FTC Act Section 5 only declared "unfair methods of competition" unlawful.[16] With its 1938 Wheeler-Lea Amendment to the FTC Act, Congress added the "unfair or deceptive acts or practices" (UDAP) prohibition, an attempt to clarify that the Commission's ambit extended to protecting consumer welfare in addition to preventing anti-competitive behavior.[17] Subsequent FTC Act amendments—the 1975 Magnuson-Moss Warranty—Federal Trade Commission Improvements Act ("Magnusson-Moss"), the 1980 FTC Improvements Act, and the 1994 FTC Reauthorization Act—altered the scope of UDAP authority and imposed heightened procedural requirements on UDAP rulemaking, but left the Commission's UMC authority unmodified.[18] As a result, neither the carve-outs to the scope of UDAP authority nor the Magnusson-Moss procedures apply when the FTC promulgates regulations under UMC.

---

[16] Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission*, 21 B.C. L. Rev. 227, 234 (1980).

[17] 52 Stat. 111. The Wheeler-Lea Amendment was a response to the Supreme Court's ruling in *F.T.C. v. Raladam Co.*, 283 U.S. 643, 649 (1931), which held that "unfair methods of competition" only reached harms to competitors.

[18] For a thorough account of this legislative history, *see* Justin (Gus) Hurwitz, *Chevron and the Limits of Administrative Antitrust*, 76 Univ. Pitt. L. Rev. 209, 232–37 (2014). Magnusson-Moss imposed additional procedural requirements on UDAP rulemaking, which the final bill text explicitly states does not apply in a UMC context. Magnuson-Moss Warranty—Federal Trade Commission Improvements Act, Pub. L. No. 93-637, 83 Stat. 2183 (1975) (codified as amended at 15 U.S.C. § 57a(a)(2) (2012)). The 1980 FTC Improvements Act modified UDAP rulemaking procedures and prohibited the Commission from regulating children's advertising under that authority, but again, as the conference report notes, left UMC rulemaking untouched. Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980) (codified at 15 U.S.C. § 57a (2012)); H.R. REP. NO. 96-917, at 1146–47. The 1994 FTC Reauthorization codified a 1980 Commission policy regarding unfair acts or practices, but did not address unfair methods of competition. Federal Trade Commission Act Amendments of 1994, Pub. L. No 103-312, 108 Stat. 1691 (1994). *See also* Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. Chic. L. Rev. 357, 377–79 (2020).

A. UMC Legal Standard

The plain text of the FTC Act, legislative history, Supreme Court precedent, and a bevy of recent academic papers on the subject all suggest the agency's UMC rulemaking authority is capacious.

The plain text of Section 5— "unfair methods of competition"—accords the FTC broad interpretive leeway: the statute offers no further definitions of the terms "unfair," "methods" or "competition." It is not a term of art, as the law's drafters specifically aimed to distinguish the clause from the common law doctrine of "unfair competition" by inserting the word "method" to create a novel construction.[19] And while "competition" connotes some sense that the unfair behavior at issue must concern an advantage one business entity gains over others,[20] this does not mean harms that primarily affect consumers necessarily lie outside the provision's reach.[21] As one antitrust scholar has put it, "it is likely that the FTC could construe any form of conduct (i.e., a 'method') that harms anyone (i.e., 'unfair') operating in the same product market as the entity engaging in that conduct (i.e., 'competition') to be an unfair method of competition."[22] In short, the agency's UMC powers are substantial.

The legislative history affirms that granting the FTC broad latitude through UMC was an intentional feature of the Commission's design. Legislators created the Commission at a moment when antitrust concerns dominated the political agenda. In *Standard Oil Co. v. United States*, 221 U.S. 1, 69–70 (1911), the Supreme Court established the rule of reason framework, ruling that

---

[19] Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 Univ. Penn. J. Bus. L. 657 (2018).
[20] This was the driving logic behind *F.T.C. v. Raladam Co.*, 283 U.S. 643, 649 (1931), since overruled.
[21] Supra note 16 at 292.
[22] Justin (Gus) Hurwitz, *Chevron and the Limits of Administrative Antitrust*, 76 Univ. Pitt. L. Rev. 263 (2014). Hurwitz also explains that under the *Chevron* doctrine, statutory ambiguity, like that on display in FTC Act Section 5, should result in judicial deference to reasonable agency interpretations.

interpreting the Sherman Act was a task reserved to the judicial branch.[23] Congressional lawmakers viewed the decision as a power grab by a Court beholden to corporate interests.[24] Many of them held a far broader understanding of the dangers posed by monopoly power and anticompetitive behavior. Their focus was not limited myopically to consumer welfare issues, but also included concerns about firms with market power extracting wealth from other producers, preserving access to open markets, and preventing the concentration of economic and political power in the hands of private corporate actors.[25]

In response to *Standard Oil*, Congress enacted the FTC Act and the Clayton Act. This dual-prong approach was intended to expand the federal government's ability to protect competition. The Clayton Act built on the Sherman Act's crime-tort model.[26] By contrast, Congress created the FTC as an expert agency, endowed it with investigatory, enforcement, and regulatory powers, and charged it to prohibit "unfair methods of competition." Its power was intended to surpass the specific prohibitions within the Sherman and Clayton Acts. Lawmakers debated whether to list prohibitions on particular types of unfair methods of competition, but ultimately decided against it. Aware that corporate actors would develop new practices to evade the letter of specific proscriptions, they sought to create a nimble agency that could adapt to new unfair behavior and go beyond the prevailing antitrust framework. In recognition of its longer reach as compared to the Sherman and Clayton Acts, the FTC Act features a narrower remedial scheme: the statute contains no private right of action and does not allow for treble damages.[27]

---

[23] Supra note 19 at 654-55.
[24] *Id.* at 655.
[25] *Id.* at 658.
[26] Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. Chic. L. Rev. 377 (2020).
[27] *Id.* at 371.

A major goal of the FTC Act was to enable the federal government to stop anti-competitive behavior in its "incipiency." Prior events taught how much more difficult it was to rein in the harmful behavior of corporations with significant market power. Many believed the Sherman Act was inadequate to address nascent threats to competition.[28] Averitt notes that the "legislative history of the Federal Trade Commission Act is replete with references which reiterate that the function of the Commission would be to arrest trade restraints in their incipiency."[29] Nascent threats to competition necessarily include a broader set of harms than the traditional antitrust harms which merit the more substantial treble damages.

The Supreme Court has also outlined, and repeatedly affirmed, a broad vision of the FTC's UMC authority. In *FTC v. R.F. Keppel & Bro.*, Inc., 291 U.S. 304, 314 (1934), the Court upheld a UMC enforcement action against a candy company that used a lottery-style marketing technique to target children under the theory that doing so granted the company an unfair competitive advantage over other candy producers who did not resort to such disreputable methods.[30] In other words, the Court affirmed that the FTC could use UMC to address anticompetitive behavior that caused consumer harm based on inappropriate targeting. When Keppel argued that only a common law anticompetitive harm or an antitrust violation, or such violation in its incipiency, could be reached using UMC, the Court retorted that, "neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories."

The Court articulated the most expansive view of the agency's UMC authority in *FTC v. Sperry & Hutchinson Co.* (1972). In that case the Supreme Court held that the statute authorized

---

[28] Supra note 19 at 662.
[29] Supra note 16 at 243.
[30] This case pre-dated the Wheeler-Lea amendment. Today, the FTC addresses consumer-facing harms through UDAP.

the agency to address anticompetitive behavior that went well beyond the narrower legal standard used by the court below to strike down the agency enforcement action at issue. The lower court held that the agency's UMC authority only reached harms that violated the "letter and spirit of the antitrust laws."[31] The *Sperry & Hutchinson* Court, upon reviewing the legislative and judicial history, disagreed. It outlined a far-reaching articulation of UMC authority:

> Thus, legislative and judicial authorities alike convince us that the Federal Trade Commission does not arrogate excessive power to itself if, in measuring a practice against the elusive, but congressionally mandated standard of fairness, it, like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws. *Federal Trade Commission v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972).

The Supreme Court reaffirmed this broad reading of the FTC's powers in *FTC v. Indiana Commission of Dentists* (1986).[32]

The seminal work on the FTC's UMC authority was written by Neil W. Averitt in 1980, who delineated five different interpretive thresholds: first, UMC reaches conduct that directly violates either the Sherman or Clayton Act; second, UMC reaches incipient violations of those statutes; third, UMC reaches conduct that violates the spirit of the antitrust laws; fourth, UMC reaches breaches of recognized competitive standards; fifth, UMC allows the FTC to "frame and enforce competition policy on its own initiative" and thus "halt any activity that results in substantial harm that results from the competitive process."[33] Averitt writes that the first three interpretations are obviously sound, while acknowledging that the fourth and fifth interpretations

---

[31] *Federal Trade Commission v. Sperry & Hutchinson Co.,* 405 U.S. 233, 245 (1972).
[32] "The standard of 'unfairness' under the FTC Act is, by necessity, an elusive one, encompassing not only practices that violate the Sherman Act and the other antitrust laws, see *FTC* v. *Cement Institute, supra*, at 689-695, but also practices that the Commission determines are against public policy for other reasons, see *Federal Trade Commission v. Sperry & Hutchinson Co.,* 405 U.S. 233, 92 S. Ct. 898 (1972); *Federal Trade Commission v. Indiana Federation of Dentists*, 476 U.S. 447, 454-55 (1986).
[33] Supra note 16 at 229.

are more tentative. In light of the legislative history, more recent scholarship has suggested that the FTC indeed possesses very broad authority.[34]

However, for the purposes of this petition it is unnecessary to fix the outer bounds of the FTC's UMC authority. The surveillance advertising business model facilitates anticompetitive behavior that fits within well-established antitrust concepts. In other words, the surveillance advertising giants—Google and Facebook—engage in activity that threatens incipient violations of the letter and spirit of the antitrust laws, and thus fits under both broad and narrow conceptions of the FTC's UMC authority.

III. BACKGROUND ON THE DIGITAL ADVERTISING ECOSYSTEM

The digital advertising market has fundamentally changed since the time Facebook emerged onto the scene in 2004. That year, out of $264 billion in total U.S. ad spending, newspapers captured $48 billion[35], while only $9.6 billion was spent online[36]—and Yahoo!'s 18% share topped the competitive digital market.[37] In 2020, Facebook and Google alone raked in roughly $108 billion of the $140 billion spent on U.S. online ads[38], while newspapers earned just $8.8 billion in ad revenue.[39] As advertising markets became primarily digital, they also fell to the trends of market tipping that favor scale and allow early winners to settle into natural monopoly positions. The rapid rise of the anticompetitive surveillance advertising giants like Google and

---

[34] Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 Univ. Penn. J. Bus. L. 645 (2018); Justin (Gus) Hurwitz, *Chevron and the Limits of Administrative Antitrust*, 76 Univ. Pitt. L. Rev. (2014); Lina M. Khan, *Amazon's Antitrust Paradox*, 126.3 The Yale Law Journal (January 2017).
[35] *Trends and Facts on Newspapers*, Pew Research Center (June 29, 2021), https://www.pewresearch.org/journalism/fact-sheet/newspapers/.
[36] *eMarketer's Seven Predictions for 2006*, eMarketer (January 11, 2006), https://www.emarketer.com/Article/eMarketers-Seven-Predictions-2006/1003773.
[37] Andrew Corn, *Google, Yahoo, AOL, MSN: Big on Internet Advertising* (March 23, 2007), https://seekingalpha.com/article/30421-google-yahoo-aol-msn-big-on-internet-advertising.
[38] Supra note 5.
[39] *Study: Newspaper Circulation Revenue Surpasses Advertising,* Associated Press (June 30, 2021), https://apnews.com/article/newspapers-business-arts-and-entertainment-ecdff2581db22fa4c627c8bfd8b48eef.

Facebook drove a stake through the heart of other traditional advertising platforms, like local news outlets, and fueled a destructive consolidation of power across markets.

There are three overarching types of digital advertising—search, display, and classified—the first two of which constitute the bulk of the total market. Broadly speaking, search consists of advertisers paying to have their ads appear alongside organic results in response to users' queries, while display consists of advertisers paying to place ads—in a variety of formats—on websites and apps whose publishers sell ad space.

Search advertising generally relies upon keywords, as opposed to profiling and personalization. However, Google has leveraged the market power and derived from its long-standing search monopoly—maintained through exclusive dealing to ensure Google is the default search engine across platforms[40]—to unfairly entrench its dominance across a significant segment of the surveillance-based display market.

In its earliest days, the display ad market functioned largely like its offline analog, with direct deals being made between advertisers and publishers. Today, the overwhelming majority of display ads are purchased through automated ("programmatic") auctions in which advertisers bid in real-time for publishers' inventory to reach targeted users on an impression-by-impression basis. In this context, having more access to users' attention, and more comprehensive data profiles on those users, are critical and mutually reinforcing competitive advantages. As such, more and more power has flowed away from publishers and advertisers, and toward dominant firms in data-rich markets such as search, social media, e-commerce, web browsing, mobile operating systems, location services, smart devices, email, and so forth.

---

[40] Bobby Allyn, *Google Paid Apple Billions to Dominate Search on iPhones, Justice Department Says,* NPR (October 22, 2020), https://www.npr.org/2020/10/22/926290942/google-paid-apple-billions-to-dominate-search-on-iphones-justice-department-says.

Display advertising can be further segmented into two distinct channels: 'owned-and-operated platforms' (closed systems), and the 'open display' market, as described by the UK's Competition and Markets Authority (CMA)[41]:

> "The owned and operated channel is primarily made up of large social media platforms, which sell their own advertising inventory directly to advertisers or media agencies through self-service interfaces. For example, an advertiser can purchase inventory directly through Facebook Ads Manager or Snapchat Ads Manager. In the open display market, a wide range of publishers (for example, including online newspapers) sell their inventory to a wide range of advertisers through a complex chain of intermediaries that run auctions on behalf of the publishers and advertisers. In practice, the largest intermediaries at each level of this complex chain are owned by a single company—Google."

As the CMA study[42] and other similar inquiries[43] show, Facebook captures an overwhelming majority of all revenue in the owned-and-operated channel.[44] Meanwhile, as extensively documented in those studies and a bevy of antitrust investigations, Google has established a vertically integrated monopoly across the entire supply chain in the open display ad market. Google simultaneously hosts most ad auctions, serves as the dominant middleman on both the buy-side and the sell-side, and competes with publishers via its own properties like YouTube, which alone generated $20 billion in advertising revenue last year.[45] To quote from the 2020 Texas-led suit against Google, "In this electronically traded market, Google is pitcher, batter, and umpire, all at the same time."[46]

In effect, Facebook and Google are both operating end-to-end marketplaces in which only they have full transparency over how prices are set, how auction winners are determined, and how

---

41 *Online platforms and digital advertising,* Competition and Markets Authority at 60 (July 1, 2021), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.
42 *Id.*
43 Australian Competition & Consumer Commission, *Digital advertising services inquiry: Interim report*, 36 (December 2020), https://www.accc.gov.au/system/files/Digital%20Advertising%20Services%20Inquiry%20-%20Interim%20report.pdf.
44 Supra note 42.
45 Alphabet Inc., Annual Report (Form 10-K), (2020), https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.
46 Supra note 8 at 2.

effective the ad buys were in reaching the targeted audiences. This opacity means that they have both the incentive and ability to rig the game to maximize their profits and mislead buyers and sellers, all without any accountability. And by restricting access to data at every step in the process, dominant firms are able to cyclically reinforce their competitive advantages—and publishers and advertisers' reliance on them—by compelling websites and apps to embed their tracking and analytics tools, through which they acquire new troves of third-party data, as the CMA explains:

> "Google and Facebook do not provide access to [consumer] data on open data exchanges, so the only way for advertisers to get (indirect) access to it and use it for targeting is to use Google and Facebook's ad management tools. As a result, third-party publishers are incentivised to use [their] advertising services. Many publishers of websites and apps also include code (tags, pixels or SDKs) that allow Google and Facebook to track the behaviour of their users to target ads and measure ad effectiveness. In doing so, third-party publishers enable Google and Facebook to obtain even more data about consumer behaviour, including on non-Google and non-Facebook properties, which further reinforces their ability to target and deliver high performing ads. Finally, both Google and Facebook do not allow advertisers and independent third-party providers of measurement and attribution services to collect user level data from ads shown on their owned and operated inventory (ie in the walled garden). This hurts independent attribution providers and gives an advantage to Google and Facebook's own ad tech and analytics services."[47]

These dynamics have set off an unwinnable race to the bottom in which a slew of market participants—including third-party providers of ad tech services and data brokers—are all desperately seeking new ways to extract and exploit user data to compete with the surveillance advertising giants. And yet, only dominant firms are positioned to succeed, as illustrated by the rapid ascent of Amazon, the only player to make real inroads since the duopoly first took shape.[48]

In addition to Amazon's unique access to first-party consumer and private business data across its many touchpoints, it has drastically expanded its access to third-party data, recently

[47] Supra note 42 at 292.
[48] Mark Sullivan, *If Anyone Can Take on Google And Facebook's Ad Duopoly, It's Amazon,* Fast Company (April 30, 2021), https://www.fastcompany.com/90631969/amazon-ad-business-growth.

passing Facebook for the number two spot in U.S. tracking reach.[49] The company boasts several significant owned-and-operated platforms beyond its main platform, including Twitch and Fire TV. And through acquisitions[50] and internal investments, it has established itself at multiple levels on both the supply and demand sides of the open display market. With these ad tech services and its unrivaled repository of consumer data, Amazon can now offer advertisers invasive new targeting options. For example, "To find people in-market for an automobile, say—even though it doesn't sell cars—Amazon has black box audience segments based on purchase data for products that often precede buying a car. Similarly, hotel brands can target Amazon audiences based on searches for terms like, say, 'travel toiletry kits.'"[51]

Facebook, Google, and Amazon now control roughly 90% of the U.S. digital ad market, and they openly cite their surveillance apparatuses as competitive advantages in corporate marketing materials:

- Amazon: "Customers rely on Amazon to browse new products, watch movies, keep up with their shows, listen to podcasts and music, and read their favorite books. These daily interactions translate to billions of first-party metrics that can help advertisers better understand the audiences that are interacting with their brand across the customer journey, both on and off Amazon."

- Facebook: "Targeting is one of the most important benefits of advertising online because it gives you the ability to show your ads to specific types of people. Keep in mind that not all digital advertising is the same, and most online advertising tools have limited targeting options... But Facebook is different. People on Facebook share their true identities, interests, life events and more."

- Google: "Engage with viewers on YouTube, Gmail and Display around important life milestones, like graduating from college, moving homes, or getting married. By

[49] Elaine Christie, *Tracking the Trackers 2020L Web Tracking's Opaque Business Model of Selling Users,* Ghostery (December 10, 2020), https://www.ghostery.com/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users/.
[50] Tim Peterson, *'Incredible Advantage': How Amazon's Sizmek Acquisition Will Address Its DSP's Weaknesses,* Digiday (June 6, 2019), https://digiday.com/marketing/incredible-advantage-amazons-sizmek-acquisition-will-address-dsps-weaknesses/.
[51] James Hercher, *The Birds-Eye View of Amazon's Advertising Business,* Ad Exchanger (June 24, 2021), https://www.adexchanger.com/online-advertising/the-birds-eye-view-of-amazons-advertising-business/.

understanding when these moments are taking place, you can tailor your advertising to reach the right users with the right messages."

IV. CASE FOR SURVEILLANCE ADVERTISING RULEMAKING

Surveillance advertising is an inherently unfair method of competition, which both relies upon, and cyclically reinforces, monopoly power. It is characterized by three distinct but interlocking categories of anticompetitive conduct: (1) the unfair extraction and monetization of data by dominant firms; (2) integration of data across business lines; and (3) exclusive dealing. This feedback loop incentivizes and facilitates increasingly anticompetitive behavior by dominant firms.

Further, as demonstrated below, the component practices cannot be disaggregated. Given the inseverable and compounding nature of these harms to competition, it is both necessary and proper for the Commission to classify surveillance advertising as an unfair method of competition in violation of the FTC Act.

A. Unfair Extraction and Monetization of Data by Dominant Firms

The surveillance advertising business model is fundamentally rooted in the widespread extraction and monetization of private data by dominant firms. In digital markets prone to tipping, data is a decisive factor in competition—and the winners tend to be rewarded with more data, further entrenching their dominance. The exploitative manner by which surveillance advertising companies wrest data from consumers and business users is both anticompetitive on its own, and is the foundation for compounding unfair practices, such as data integration across business lines and exclusive dealing to actively suppress competition.

Most people did not, and would not, willingly sign up to be spied on across the internet—or hand over the full suite of personal and behavioral information major platforms now extract

from them—for corporate gain. Rather, the dominant firms that engage in surveillance advertising originally enticed them with 'free' high-quality products, idealistic visions, and stronger privacy policies in order to gain market share, and once users were locked in, effectively hiked prices on them by eroding privacy and otherwise degrading services. In a competitive marketplace with ample choices and minimal switching costs, few consumers would agree to simply continue paying more for less. Nor would publishers and advertisers willingly relinquish valuable data about their own customers to be tracked across the internet by dominant firms with whom they compete. This is only possible because of escalating abuses of monopoly power made possible by surveillance advertising.

This data extraction, which is the lifeblood of the surveillance advertising business model, creates a vicious cycle of distorted competition. Dominant firms are able to lock in users and subsequently extract large amounts of personal and behavioral data. With the extensive profiles they cultivate on each user, and the aggregate behavioral insights they glean, these platforms can then feed users hyper-personalized content engineered to keep them clicking. In turn, they can then increase costs on publishers and advertisers for precisely targeted ad space, while also increasing costs for captive users in the form of expanded data extraction. They can do this while simultaneously degrading product quality, from increasing the prevalence of ads across the platform and diminishing user control, to further eroding privacy protections and algorithmically amplifying extreme and dangerous content.

Thus, surveillance advertising is both foundationally and cyclically anticompetitive: It allows dominant firms to continuously extract more data and profit from trapped users, while raising barriers to entry that serve to further deprive those users of viable alternatives.

1. *Competitive Constraints Initially Prevented Today's Dominant Surveillance Advertising Firms From Engaging in Unfair Data Extraction and Monetization Practices*

In 2005, one year after Facebook launched, the platform's privacy policy promised that "we do not and will not use cookies to collect private information from any user."[52] It was a promise the company did not keep. In 2020, Facebook generated more than $85 billion in revenue, largely by collecting data about users' activities, interests, and affiliations to sell invasive advertisements.[53]

Yet, Facebook's ostensible commitment to privacy in its incipiency—in addition to a series of anticompetitive practices outlined below—played a key role in tipping the market in the platform's favor. Even after walking back its initial promise to not collect any private data, early Facebook privacy policies gave users the ability to opt out of having their information shared *with* third parties, including advertisers and marketers; allowed users to prohibit the platform from collecting personal information *from* third parties; and allowed users to modify or remove information Facebook had about them at any time.[54] These policies played an important role in attracting consumers to the platform, particularly as Myspace—the market leader at the time—was beset by burgeoning concerns over its failures to protect users.[55] In 2006, Myspace had 100 million users to Facebook's 12 million.[56] But in 2007, user growth at Myspace started to decelerate, while

---

[52] Facebook, *[The Facebook] Privacy Policy,* Facebook Web Archive (2005), https://web.archive.org/web/20050107221705/http://www.thefacebook.com/policy.php.
[53] Statista Research Department, *Facebook: Advertising Revenue Worldwide 2009-2020,* Statista (February 5, 2021), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/.
[54] Dina Srinivasan, *The Antitrust Case Against Facebook,* Berkeley Business Law Journal Volume 16, Issue 1 at 51, (Jan. 19, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247362.
[55] Gary D. Robertson, *Myspace: 29,000 Sex Offenders Have Profiles,* NBC News (July 24, 2007), https://www.nbcnews.com/id/wbna19936355.
[56] *Number of Active Users at Facebook Over the Years*, The Associated Press (October 23, 2012), https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html.

growth at Facebook rapidly accelerated until, by midyear, Facebook had overtaken Myspace as the most visited social media network in the U.S.[57]

With budding momentum in the market, Facebook reneged on the promise not to surveil user activity outside of Facebook with the release of an advertising product called "Beacon" in November 2007.[58] Beacon was a direct product license to third-parties that allowed Facebook to monitor and record user activity on the sites of independent businesses.[59] The market, which at this point was still relatively competitive, reacted swiftly. A MoveOn.org petition garnered 50,000 signatures within days;[60] class-action lawsuits on behalf of users were filed in Texas and California;[61] and national news articles highlighted users' privacy concerns.[62] With numerous rivals in the social networking space, Facebook retreated; less than a month after launching Beacon, Zuckerberg issued a public apology, saying "Facebook has succeeded so far in part because it gives people control over what and how they share information."[63] With Beacon, Zuckerberg noted, Facebook "missed the right balance."[64]

On the heels of the Beacon controversy, and competitors' rising awareness of the importance of privacy to consumers, Facebook took the unprecedented step of announcing that future privacy changes would be subject to user approval.[65] In a rare press conference, Zuckerberg

---

[57] Erick Schonfeld, *Facebook Blows Past Myspace in Global Visitors for May*, TechCrunch (June 20, 2008), https://techcrunch.com/2008/06/20/facebook-blows-past-myspace-in-global-visitors-for-may/.
[58] Michael Arrington, *Ok Here's At Least Part of What Facebook Is Announcing on Tuesday: Project Beacon,* TechCrunch (November 2, 2007), https://techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday/.
[59] Supra note 54 at 56.
[60] Nick O'Neill, *MoveOn.org to Challenge Facebook Beacon*, AdWeek (November 20, 2007), www.adweek.com/digital/moveonorg-to-challenge-facebook-beacon/.
[61] Harris v. Blockbuster Inc., 622 F. Supp. 2d 396 (N.D. Tex. 2009); Lane v. Facebook Inc., 696 F.3d 811 (9th Cir. 2012).
[62] Eric Auchard, *Facebook Alters Notifications after Privacy Furor*, Reuters (November 29, 2007), https://www.reuters.com/article/us-facebook-privacy-idUSN2925736120071130.
[63] Mark Zuckerberg, *Thoughts on Beacon*, Facebook Blog (December 5, 2007), https://web.archive.org/web/20080107025500/http://blog.facebook.com/blog.php?post=7584397130.
[64] *Id.*
[65] Supra note 54 at 61.

explained Facebook was "making it so that we can't just put in a new terms of service without everyone's permission. We think these changes will increase the bonding and trust users place in the service."[66]

Even as the company publicly doubled down on its commitment to privacy, Facebook began laying a far more extensive foundation for surveillance that it could eventually deploy if and when its market position allowed. The target this time was not Facebook users, but the thousands of publishers that competed with Facebook for digital ad dollars. In the wake of Facebook's Beacon retreat, the company introduced 'social plugins':

> "The relevant history of Facebook social plugins centers around the 'Like' button—introduced early in 2010... For publishers, the Like buttons offered a turn-key review and distribution mechanism. Facebook explained, '[e]ach Like creates distribution on Facebook, which brings more Facebook users back to the article on your site.' Because online publishers generate incremental revenue for each click on an article, more user visits meant more money."[67]

Thousands of publishers installed the Facebook Like button. But like Beacon before it, social plugins required independent businesses to install Facebook code on their websites, which created "a backdoor communication between users' devices and Facebook's servers."[68] When Zuckerberg first announced the Like button at a 2010 developer's conference, he did not mention this opening that could eventually be used by Facebook to track users across the internet. After this fact came to light—fearing another Beacon-like backlash in what was then still a competitive market—Facebook repeatedly asserted it would not leverage that access for commercial gain.[69] This deception was critical to soliciting the coordination of third-parties to integrate Facebook code into their websites:

---

[66] *Id.* at 62.
[67] *Id.*
[68] *Id.* at 63.
[69] *Id.*

> "Many third-parties, publishers for example, competed with Facebook on the advertising side of the market. They licensed and installed social plugins as a means to distribute their own content. Surveillance of their own readers, however, could be used against them to undercut the value of and pricing power over their own proprietary readers. Specifically, if Facebook could compile a list of people that read the [Wall Street] Journal, even those who did not use Facebook, it could simply sell the ability to retarget "Journal readers" with ads across the internet for a fraction of the cost that the Journal charged...Proprietary access to subscribers and the identities of readers and visitors is a highly guarded asset historically by subscription businesses. It is unlikely that publishers would have shared this information unless they were under the belief that Facebook was a content distribution platform and traffic generator, not a surreptitious aggregator of consumer data for Facebook's own internal, and competitive, advertising sales efforts."[70]

To continue increasing its market share and convince publishers to embed the code, Facebook was forced to keep up the privacy charade until it secured a dominant position and was free to act without competitive constraints, as detailed in subsequent sections.

Google followed a similar playbook. The search engine giant built its empire and gained footholds in a slew of digital markets by marketing 'free' products that promised to protect user privacy. For years, users took comfort in the fact that the company kept the sensitive data they generated on distinct Google-owned properties and services largely compartmentalized. For example, when Google bought the ad server DoubleClick in 2007, Google founder Sergey Brin said that privacy would be the company's "number one priority when we contemplate new kinds of advertising products."[71] For nearly a decade, Google kept DoubleClick's massive database of web-browsing records separate by default from the names and other personally identifiable information Google collected from Gmail and its other login accounts.[72] At the time of the purchase in 2007, for example, Google's privacy policy stated, "DoubleClick's ad-serving technology will

[70] *Id.* at 64, 72.
[71] Julia Angwin, *Google's Broken Privacy Promise,* Pacific Standard (June 14, 2017), https://psmag.com/news/googles-broken-privacy-promise.
[72] *Id.*

be targeted based only on the non-personally-identifiable information."[73] This commitment was not just made to the public, it was made to Congress and the FTC.[74]

Into the 2010s, Google continued promising privacy protections to the public and the government. In August 2010, a tech watchdog released proof that Google had impeded users who tried to opt out of data collection. One week later, Google announced that it had made its privacy policy "more transparent and understandable" by eliminating legal jargon and repetitive sentences without damaging users' privacy.[75] The change allowed Google to draw attention away from watchdog accusations and demonstrate their commitment to data security. Google's policy change, however, contained an ulterior motive. According to Marc Rotenberg of the Electronic Privacy Information Center, the change laid the groundwork for Google to break privacy promises in the future.[76] Previously, Google had different rules for different products (Search, Google+, Android, etc.). The shorter policy generalized its rules for all products, creating loopholes for Google to acquire data[77] and build unified superprofiles on users, as discussed further in subsequent sections. Nevertheless, Google perversely held up this change as proof of its devotion to privacy, testifying at a congressional hearing in January 2012 that the streamlined policy was a "great example" of their commitment to "providing transparency, control, and security to our users."[78]

2. *After Locking Users In, Dominant Platforms Increased Prices On Consumers, Advertisers, And Publishers, Through Increased Data Extraction and Degraded Services*

---

[73] *Id.*
[74] Supra note 3.
[75] Google, *Trimming Our Privacy Policies,* Official Blog (September 3, 2010), https://googleblog.blogspot.com/2010/09/trimming-our-privacy-policies.html.
[76] Nick Bilton, *Google to Simplify Its Privacy Policies,* The-Dispatch.com (September 8, 2010), https://www.the-dispatch.com/news/20100903/google-to-simplify-its-privacy-policies/1.
[77] *Id.*
[78] Pablo Chavez, *Letter to Members of Congress regarding Privacy Policy,* Google (January 30, 2012), https://drive.google.com/file/d/0BwxyRPFduTN2NTZhNDlkZDgtMmM3MC00Yjc0LTg4YTMtYTM3NDkxZTE2OWRi/view?resourcekey=0-S-YxsyPhvImsBdpzmyPohw.

Surveillance advertising can only flourish in an unhealthy market, and once it takes hold, it further degrades market quality and competition. When consumers and other market participants can vote with their feet, competitive forces restrain firms from engaging in the mass-extraction and monetization of user data. This is evidenced by Facebook's initial retreat on products like Beacon, and Google's promised firewall between DoubleClick and its touchpoints that yielded personally identifiable information. But once a market tips—as digital markets tend to do—dominant firms are unshackled, free to accelerate the surveillance advertising flywheel.

That's exactly what happened with Facebook. In 2012, Facebook went public, and by early 2014, rivals that initially competed with Facebook had been forced out of the market, including Myspace, Friendster, AOL's Bebo, and dozens of others.[79] As experts have noted, "For Facebook, these circumstances—the exit of competition and the lock-in of consumers—greenlit a change in conduct."[80]

In December 2012, Facebook abolished the ability of users to block privacy changes via referendum.[81] In 2014, after representing that it would not use social widgets to track consumers, Facebook announced it would track users on third-party sites and apps that had installed Facebook plugins.[82] And later in 2014, Facebook further deteriorated user privacy by tying the newly announced tracking of consumer behavior across the web to personal identities known through its dominant personal social networking service.[83] These changes enabled Facebook to build comprehensive data profiles on each user, micro-target them, and auction off their attention to the highest advertising bidder.

---

[79] Supra note 54 at 69.
[80] *Id.* at 70.
[81] Dan Farber, *The Facebook Vote and a Nation-State in Cyberspace,* CNET (December 11, 2012), https://www.cnet.com/tech/services-and-software/the-facebook-vote-and-a-nation-state-in-cyberspace/#.
[82] Geoffrey A. Fowler, *There's No Escape from Facebook, Even If You Don't Use It,* The Seattle Times (August 31, 2021), https://www.seattletimes.com/business/technology/theres-no-escape-from-facebook-even-if-you-dont-use-it/.
[83] Supra note 54 at 73.

Facebook's change in data extraction and monetization practices amounts to a massive price hike on users. Every additional unit of data that Facebook coercively procures from its users is valuable currency that users are functionally being forced to pay. Perhaps the best way to quantify the magnitude of this is by using Facebook's own key metric: "average revenue per user" (ARPU). As stated in its SEC filings, Facebook generates "substantially all" of its revenue from selling advertisers targeted access to users' data profiles. Over the first two quarters of 2011, Facebook earned an average of roughly $5 per American user.[84] Over Q1 and Q2 of 2021, that ARPU shot up to $101.[85] That is to say, by this measure, Facebook has exploited its monopoly power to subject Americans to a 20-fold price hike over the past decade.

Consumers are not the only parties unable to rebuff these increasingly aggressive data extraction practices; businesses—including publishers and advertisers—have suffered similar fates. By 2014, "Facebook had a substantial portion of the horizontal market coordinating with it for some functionality or another—whether for user registration or article sharing."[86] These publishers had built their businesses over the last seven years to depend on Facebook code, and now, that reliance was correlated with their own ability to generate revenue.[87] Simply put: they could not escape. This has allowed Facebook to extract monopoly prices. The cost per mille (CPM) – a common measurement for digital ad-buying – for Facebook has increased 89% year over year as of July 2021, and its average price per ad has increased 47% year over year with more hikes expected soon.[88]

---

[84] Facebook Inc., Annual Report (Form 10-K), (2012), https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_2012_10K.pdf.
[85] Facebook Inc., Annual Report (Form 10-K), (2020), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf.
[86] *Id.*
[87] *Id.*
[88] Lauren Johnson, *Facebook, Google, and Amazon Are Having a Banner Year And It's Causing Ad Prices to Spike – Here's Exactly How Much,* Business Insider (August 2, 2021), https://www.businessinsider.com/facebook-google-amazon-advertising-break-down-ad-prices-2021-7.

By increasing prices on users, publishers, and advertisers, Facebook's digital ad revenue nearly doubled between 2013 and 2014: from $6.9 billion to $11.5 billion.[89] In a 2018 earnings call, Dave Wehner, Chief Financial Officer of Facebook, admitted Facebook's ability to extract user data is directly tied to higher behavioral advertising revenues.[90] He was right: As the platform's data advantage compounded over time, Facebook extracted more and more data with no competitive consequences. As a result, the company's revenues surged. In Q1 of 2021 alone, Facebook posted $26.17 billion in revenue, which the company attributed to "a 30% increase in the average price per ad, as well as a 12% increase in the number of ads shown."[91]

Again, Google followed a similar trajectory after sufficiently locking consumers and business users into its sprawling ecosystem of products across key digital markets. Google continued to play up its feel-good image as a quirky search startup from Silicon Valley even as it was becoming ubiquitous and attracting widespread antitrust scrutiny,[92] including a then-record FTC fine in 2012 for misrepresenting its surveillance advertising policies.[93] Today, *nine* of Google's products—Android, Chrome, Gmail, Google Search, Google Drive, Google Maps, Google Photos, Google Play Store, and YouTube—have more than a billion users each.[94]

In a span of 20 years, Google bought up well over 260 companies.[95] Among the acquisitions were its DoubleClick ad server and a slew of other ad tech tools that collectively laid the

---

[89] Statista Research Department, *Facebook: Advertising Revenue Worldwide 2009-2020,* Statista (February 5, 2021), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/.
[90] Facebook Inc., Q2 2018 Earnings Conference Call, (July 25, 2018), https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q218-earnings-call-transcript.
[91] Salvador Rodriguez, *Facebook Revenue Rises 48%, Driven By Higher-Priced Ads,* CNBC (April 28, 2021), https://www.cnbc.com/2021/04/28/facebook-fb-earnings-q1-2021.html.
[92] Claire Cain Miller, *Google Bases a Campaign on Emotions, Not Terms*, The New York Times (January 1, 2012), https://www.nytimes.com/2012/01/02/technology/google-hones-its-advertising-message-playing-to-emotions.html.
[93] Federal Trade Commission, *Google Will Pay $225 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser,* Press Release (August 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
[94] *Id.*
[95] Supra note 3.

groundwork for a vertically integrated monopoly across the open display supply chain. Key purchases included mobile ad network AdMob in 2009, demand-side platform Invite Media in 2010, supply-side platform and real-time bidding tool AdMeld in 2011, and analytics and attribution provider Adometry in 2014.[96]

In 2016, having established dominant positions throughout the digital economy and ad tech stack, Google removed the firewall between DoubleClick browsing data and the personal data collected through its other platforms, breaching a decade-old promise to users. The privacy policy that once stated DoubleClick technology "will be targeted based only on the non-personally-identifiable information,"[97] was changed to state, "your activity on other sites and apps may be associated with your personal information."[98] While users could still technically opt out of these trackers through their settings, most were unaware of this change that supercharged Google's surveillance advertising monopoly power.

At a 2020 House Antitrust Subcommittee hearing, Rep. Val Demings (D-FL) questioned Google CEO Sundar Pichai about the DoubleClick reversal,[99] noting that in 2007, Google's founders were concerned that combining the data would lead to a privacy backlash:

> "So, in 2007, Google's founders feared making this change because they knew it would upset their users, but in 2016, Google didn't seem to care. Mr. Pichai, isn't it true that what changed between 2007 and 2016 is that Google gained enormous market power. So. While Google had to care about user privacy in 2007. It no longer had to in 2016? Would you agree that what changed was Google gained enormous market power?"[100]

---

96 Supra note 41 at 272.
97 Julia Angwin, *Google's Broken Privacy Promise,* PacificStandard (June 14, 2017), https://psmag.com/news/googles-broken-privacy-promise.
98 *Id.*
99 Justin Wise, *Val Demings Repeatedly Presses Google's Pichai On 'Staggering' Consolidation of Consumer Data*, The Hill (July 29, 2020), https://thehill.com/policy/technology/509642-val-demings-repeatedly-presses-googles-pichai-on-consolidation-of-consumer.
100 Supra note 3.

Google's policy change allowed the company to further monetize user data and served as an effective price hike on users in the form of decreased privacy (i.e. by creating "deeper and deeper profiles of consumers' internet activity").[101] But users were not the only group that faced higher prices after Google obtained sufficient market power. Like Facebook, Google was also able to increase prices on advertisers and publishers. Google's CPM associated with its programmatic inventory increased 198% year over year in July 2021.[102] And in a lawsuit filed by ten state attorneys general in December 2020, prosecutors claimed that "Google overcharged publishers for the ads it showed across the web and edged out rivals who tried to challenge the company's dominance,"[103] both of which were made possible by Google's unfair data extraction and monetization practices.

Despite these price increases, smaller stakeholders are now forced to rely on the dominant surveillance advertising firms and the black-box marketplaces they operate for everything from distribution and targeting, to pricing and analytics. Google has thus been free to extract monopoly fees from them and gain competitive intelligence from their unique audience data, among other abuses; the only alternative is losing access to the digital economy. These data extraction and monetization practices stifle competition, and have a cascading effect across digital markets, as other ad tech providers and would-be rivals feel obliged to emulate the unscrupulous standards they've set, or fall even further behind. Meanwhile, Google's digital ad revenue has soared from $59.62 billion in 2014 to $146.92 billion in 2020.[104]

---

[101] Supra note 54.
[102] Lauren Johnson, *Facebook, Google, and Amazon Are Having a Banner Year And It's Causing Ad Prices to Spike – Here's Exactly How Much,* Business Insider (August 2, 2021), https://www.businessinsider.com/facebook-google-amazon-advertising-break-down-ad-prices-2021-7.
[103] David McCabe and Daisuke Wakabayashi, *10 States Accuse Google of Abusing Monopoly in Online Ads,* The New York Times (December 16, 2020), https://www.nytimes.com/2020/12/16/technology/google-monopoly-antitrust.html.
[104] Joseph Johnson, *Google: Annual Advertising Revenue 2001-2020,* Statista (February 5, 2021), https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

a) Additional Consumer and Societal Harms from Surveillance Advertising Platforms

Beyond the aforementioned cost increases in the form of privacy reductions, dominant firms have inflicted upon consumers and society a litany of significant harms as a consequence of, and in furtherance of, their surveillance advertising businesses. In zero-price digital markets, each of these breaches of privacy and degradation in quality of services constitutes an effective price hike—and each further exacerbates their ability and incentive to perpetuate more harm and extract more profits. On the one hand, this list is far from exhaustive; on the other, any one of these enumerated harms—and certainly, their cumulative toll—would cause significant user flight in a healthy marketplace. Dominant surveillance advertising firms are only able to continue engaging in such conduct without repercussions, and indeed, to greater profits, due to their monopoly power.

i) Perpetuating Discrimination

Dominant surveillance advertising firms have repeatedly facilitated discriminatory targeting of ads for employment, housing, and financial services on the basis of race, religion, and gender in violation of civil rights laws.[105] Worse, in many cases, these harms are not merely the result of inappropriate targeting categories, but fundamentally baked into their algorithms.[106] For example, after Facebook was forced to settle with HUD over housing ads that explicitly excluded

[105] Julia Carpenter, *Google's Algorithm Shows Prestigious Job Ads to Men, But Not to Women. Here's Why That Should Worry You,* The Washington Post (July 6, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/07/06/googles-algorithm-shows-prestigious-job-ads-to-men-but-not-to-women-heres-why-that-should-worry-you/; Rory Cellan-Jones, *Facebook Accused of Allowing Sexist Job Advertising,* BBCNews (September 9, 2021), https://www.bbc.com/news/technology-58487026; Karen Hao, *Facebook's Ad Algorithms Are Still Exclusing Women From Seeing Jobs,* MIT Technology Review (April 9, 2021), https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination/; Jeremy B. Merrill, *Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads,* The Markup (Febrary 11, 2021), https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads.

[106] Alex P. Miller and Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias,* Harvard Business Review (November 8, 2019), https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias.

individuals by race and other protected characteristics,[107] and announced changes to ostensibly fix the problem,[108] their algorithm continued to perpetuate that bias regardless of advertisers' efforts to target diverse audiences.[109] Because the surveillance advertising business model creates such unavoidable dominance, Facebook and other platforms can actively disregard user demands—including calls to not discriminate based on race or gender—without worrying about user flight.

ii) Exploiting Kids and Teens

In its relentless pursuit of maximizing data extraction and monetization, Facebook tagged hundreds of thousands of children as being "interested in" targeted advertisements for gambling and alcohol,[110] and has similarly greenlit ads targeting minors that promote anorexia, smoking, and pill abuse.[111] Google and YouTube, meanwhile, paid a record $170 million settlement to the FTC for illegally collecting children's personal information without consent[112]—and YouTube's engagement and profit-driven recommendation algorithm was even found to be feeding videos of partially clothed children to pedophiles.[113] Most recently, the Wall Street Journal reported that Facebook executives refused to act on extensive internal research showing that Instagram fueled teen depression, noting that, "Expanding its base of young users is vital to the company's more

---

[107] Charge of Descrimination, *Dept. Housing and Urban Development. v. Facebook Inc,* FHEO No. 01-18-0323-8J at 6 (August 13, 2018), https://archives.hud.gov/news/2019/HUD_v_Facebook.pdf.
[108] Facebook for Business, *Updates to Housing, Employment and Credit Ads in Ads Manager,* Facebook Newsroom (August 26, 2019), https://www.facebook.com/business/news/updates-to-housing-employment-and-credit-ads-in-ads-manager.
[109] Molly Callahan, *Facebook Changed Its Ad Tools, But the Results Are Still Biased. What's Going On?,* News@Northeastern (December 18, 2019), https://news.northeastern.edu/2019/12/18/facebooks-ad-delivery-system-still-discriminates-by-race-gender-age-y/.
[110] Alex Hern and Frederik Hugo Ledegaard, *Children 'Interested In' Gambling and Alcohol, According to Facebook,* The Guardian (October 9, 2019), https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook.
[111] *Pills, Cocktails, and Anorexia: Facebook Allows Harmful Ads to Target Teens,* Tech Transparency Project (May 4, 2021), https://www.techtransparencyproject.org/articles/pills-cocktails-and-anorexia-facebook-allows-harmful-ads-target-teens.
[112] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FTC (September 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.
[113] Max Fisher and Amanda Taub, *On YouTube's Digital Playground, an Open Gate for Pedophiles,* The New York Times (June 3, 2019), https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html.

than $100 billion in annual revenue, and it doesn't want to jeopardize their engagement with the platform."[114] The ability and incentive to extract more user data to unfairly monetize, even at the expense of children's wellbeing, has proven too great a competitive advantage for dominant surveillance advertising firms to pass up.

iii) Fueling Extremism

To a similar end, Facebook has tagged users as being interested in Nazis and allowed advertisers to directly target them,[115] aimed ads for tactical military gear at insurrectionists,[116] and run targeted recruitment ads for dangerous militia groups organizing on its platform.[117] Both Facebook and YouTube's recommendation algorithms—operating on the same infrastructure and incentives as their ad targeting tools—played a critical role in mainstreaming the QAnon movement.[118] And even when more than 1,000 advertisers boycotted Facebook for profiting off hate, Mark Zuckerberg told staff that they'd "be back on the platform soon enough," underscoring the company's monopoly power.[119] For surveillance advertising firms, boosting outrageous content and pushing users into rabbit holes of radicalization drives more engagement, captures more user data and attention, and allows them to serve more invasive ads. In competitive markets, such data

---

[114] Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, *Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show,* The Wall Street Journal (September 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.
[115] Sam Dean, *Facebook Decided Which Users Are Interested in Nazis –And Let Advertisers Target Them Directly,* Los Angeles Times (Febrary 21, 2019), https://www.latimes.com/business/technology/la-fi-tn-facebook-nazi-metal-ads-20190221-story.html.
[116] Ryan Mac and Craig Silverman, *Facebook Has Been Showing Military Gear Ads Next to Insurrection Posts*, Buzzfeed News (January 13, 2021), https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot.
[117] *Facebook Ran Recruitment Ads for Militia Groups,* Tech Transparency Project (October 19, 2020), https://www.techtransparencyproject.org/articles/facebook-ran-recruitment-ads-militia-groups.
[118] Julia Carrie Wong, *Down the Rabbit Hole: How QAnon Conspiracies Thrive on Facebook,* The Guardian (June 25, 2020), https://www.theguardian.com/technology/2020/jun/25/qanon-facebook-conspiracy-theories-algorithm.
[119] Alex Heath, *Zuckerberg Tells Facebook Staff He Expects Advertisers to Return 'Soon Enough',* The Information (July 1, 2020), https://www.theinformation.com/articles/zuckerberg-tells-facebook-staff-he-expects-advertisers-to-return-soon-enough.

collection and monetization practices would at the least, incentivize backlash and entry by other firms with less exploitative business models.

iv) Amplifying Misinformation

The surveillance advertising platforms have also allowed targeting ads based on users' interest in 'pseudoscience' to spread false conspiracy theories about the transmission of COVID-19 and promote anti-vaccine hoaxes, posing a direct harm to public health.[120] Facebook executives, presented with data showing their algorithms amplify toxic misinformation, have repeatedly shot down remedies that would limit surveillance advertising revenue.[121] And Google's programmatic ad tech services have financed medical misinformation sites,[122] election lies,[123] and Russian propaganda.[124]

Due to the monopoly power of these surveillance advertising giants, rather than sparking the sort of consumer exodus and financial ramifications that would be expected in a healthy market, this deluge of harms has only driven even more profit, entrenched their dominance, and further insulated them from public pressure. In fact, after a recent string of particularly damning stories, the New York Times reported that, "For years, Facebook confronted crisis after crisis over privacy, misinformation and hate speech on its platform by publicly apologizing," but have moved on to

---

[120] Meria Gebel, *Anti-vaccination Ads on Facebook Are Targeting Pregnant Women, While a Measles Outbreak Spreads Across the Country,* Business Insider (February 14, 2019), https://www.businessinsider.com/anti-vaccine-facebook-ads-target-pregnant-women-as-measles-spreads-2019-2; Paige Leskin, *Facebook Let Advertisers Target Users Interested in 'Pseudoscience', Allowing Them to Capitalize on Conspiracy Theories That Falsely Blame 5G Cell Towers for the Coronavirus,* Business Insider (April 23, 2020), https://www.businessinsider.com/facebook-ads-target-pseudoscience-conspiracy-theories-coronavirus-5g-misinformation-report-2020-4.

[121] Keach Hagey and Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead,* The Wall Street Journal (September 15, 2021), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

[122] Christian Fleetwood, *Over 4,000 Brands Bought Programmatic Ads on COVID-19 Misinformation Websites*, BandT.com (February 19, 2021), https://www.bandt.com.au/over-4000-brands-bought-programmatic-ads-on-covid-19-misinformation-websites/.

[123] Issie Lapowsky, *Google Says It's Fighting Election Lies, But Its Programmatic Ads Are Funding Them,* Protocol (January 14, 2021), https://www.protocol.com/google-programmatic-ads-misinformation.

[124] L. Gordon Crovitz, *Opinion | How Amazon, Geico, and Walmart Fun Propaganda,* The New York Times (January 21, 2020), https://www.nytimes.com/2020/01/21/opinion/fake-news-russia-ads.html.

an aggressive new strategy that omits remorse and instead relies on artificially amplifying pro-Facebook stories on its own platform.[125]

b) Additional Competitive Harms to Captive Publishers and Advertisers

Degrading quality of services has not been confined to users. Surveillance advertising has also positioned dominant firms to provide deceitful metrics to publishers and advertisers, and otherwise capitalize on their lack of choice, bargaining power, and access to data. For example, in 2016, Facebook was caught misreporting metrics it used to price its advertising services to publishers, exaggerating its "average viewing time" metric by as much as 80%.[126] In 2017, they were caught claiming they reached millions more U.S. users in key age groups than even resided in the country, per official census data.[127] In 2018, they were sued for knowingly inflating ad-watch times by up to 900%, effectively defrauding advertisers.[128] Recently unsealed court documents revealed a Facebook product manager bemoaning "revenue we should have never made given the fact it's based on wrong data,"[129] and the company's longtime head of global ad sales admitting that their fraudulent metrics "clearly impacted [advertisers'] planning."[130] Internal Facebook documents also show managers admitting to flaws in its surveillance advertising targeting

[125] Ryan Mac and Sheera Frenkel, *No More Apologies: Inside Facebook's Push to Defend Its Image*, New York Times (September 21, 2021), https://www.nytimes.com/2021/09/21/technology/zuckerberg-facebook-project-amplify.html.
[126] Lara O'Reilly, *Facebook Admits It Exaggerated Ad Metrics,* Inc. (November 17, 2016), https://www.inc.com/business-insider/facebook-ad-metrics-exaggeration-update.html.
[127] Lara O'Reilly, *Facebook's Claimed Reach in the U.S., Is Larger Than Census Figures, Analyst Finds,* The Wall Street Journal (September 6, 2017), https://www.wsj.com/articles/facebooks-claimed-reach-in-the-u-s-is-larger-than-census-figures-analyst-finds-1504711935.
[128] Ethan Baron, *Facebook Lured Advertisers by Inflating Ad-Watch Times by Up To 900%: Lawsuit*, Mercury News (October 16, 2018), https://www.mercurynews.com/2018/10/16/facebook-lured-advertisers-by-inflating-ad-watch-times-up-to-900-percent-lawsuit/.
[129] Hannay Murphy, *Facebook Reported Revenue It 'Should Have Never Made', Manager Claimed,* Financial Times (February 18, 2021), https://www.ft.com/content/c144b3e0-a502-440b-8565-53a4ce5470a5.
[130] *Facebook Advertising Chief Worried About Whether It Overstated Audience,* The Irish Times (April 26, 2021), https://www.irishtimes.com/business/technology/facebook-advertising-chief-worried-about-whether-it-overstated-audience-1.4548113.

capabilities that resulted in ads reaching their intended audiences less than half the time, with one Facebook manager dismissing the company's own targeting data as "all crap."[131]

In the Google-dominated open display channel, publishers and advertisers have faced similar quality degradations and asymmetries of knowledge. Beyond the "monopoly tax on billions of daily transactions" that Google charges participants across the supply chain, and the flagrant market-rigging and self-dealing discussed later in this petition, publishers and advertisers suffer from widespread fraud,[132] unviewable ads,[133] significant brand safety risks, audience leakage, and more. The automated exchanges—which run through an opaque series of ad tech intermediaries that consume up to half of total ad spend—leave buyers and sellers alike with little control or insight into the process. Google's push for greater monetization of its surveillance data streams has led major advertisers and family-friendly brands to inadvertently fund and appear next to dangerous medical hoaxes,[134] fringe outlets that stoked the Capitol insurrection,[135] and foreign propaganda[136] among other things. Compounding matters, advertisers seeking to avoid this brand damage often resort to broad keyword blocklists that exclude their content from appearing near words like 'racism,' which perversely ends up defunding legitimate news publishers.[137] It's a

---

[131] Sam Biddle, *Facebook Managers Trash Their Own Ad Targeting in Unsealed Remarks,* The Intercept (December 24, 2020), https://theintercept.com/2020/12/24/facebook-ad-targeting-small-business/.
[132] Michelle Castillo, *Online Ad Fraud is a 'Widespread' Problem, Google and Other Big Ad Platforms Admit,* CNBC (July 21, 2017), https://www.cnbc.com/2017/07/21/google-oath-others-ad-fraud-widespread-problem.html.
[133] Lara O'Reilly, *Google Just Admitted More Than Half of the Ads It Serves Are Never Seen,* Business Insider (December 3, 2014), https://www.businessinsider.com/google-display-ad-viewability-study-2014-12.
[134] Ryan Gallagher and Mark Bergen, *Google Helps Place Ads on Sits Amplifying COVID-19 Conspiracies,* Bloomberg (June 1, 2020), https://www.bloomberg.com/news/articles/2020-06-01/google-helps-place-ads-on-sites-amplifying-covid-19-conspiracies.
[135] Abram Brown, *How 'Gateway Pundit' Used Vaccine and Election Misinformation To Earn $1.1 Million in Google Ad Revenue,* Forbes (July 29, 2021), https://www.forbes.com/sites/abrambrown/2021/07/29/gateway-pundit-election-vaccine-covid-misinformation-google/.
[136] L. Gordon Crovitz, *Opinion | How Amazon, Geico, and Walmart Fun Propaganda,* The New York Times (January 21, 2020), https://www.nytimes.com/2020/01/21/opinion/fake-news-russia-ads.html.
[137] Jeff Beer, *The Attempted Coup At the Capitol Needs to be Brands' Wake-up Call About Funding Online Disinformation,* Fast Company (January 8, 2021), https://www.fastcompany.com/90592199/the-capitol-coup-needs-to-be-brands-wake-up-call-about-funding-online-disinformation.

similar plight to the one suffered by hundreds of small business owners wrongly purged from Facebook in errant AI crackdowns, with many left to wait months for service because only advertisers who spend $10,000 per month receive dedicated customer service representatives.[138]

And then there's the problem of audience theft—whereby surveillance advertising enables outlets' readership to be extrapolated and targeted elsewhere at lower costs—captured in this anecdote from Recode cofounder Walt Mossberg:

> "About a week after [Recode's] launch, I was seated at a dinner next to a major advertising executive. He complimented me on our new site's quality and on that of a predecessor site we had created and run, AllThingsD.com. I asked him if that meant he'd be placing ads on our fledgling site. He said yes, he'd do that for a little while. And then, after the cookies he placed on Recode helped him to track our desirable audience around the web, his agency would begin removing the ads and placing them on cheaper sites our readers also happened to visit."[139]

At every turn, this exploitation by dominant surveillance advertising firms simultaneously harms publishers and advertisers, while making them even more dependent upon the digital gatekeepers, who extract more user data, competitive insights, and profit. Despite increasing harms to their own customers, the surveillance advertising giants do not face substantial competition. Instead, because of the superior resources derived from this business model, the dominant firms are able to further entrench their position, building bigger products and seizing on scale advantages that are not available to others.

---

[138] Tyler Sonnemaker, *Facebook's AI-fueled Attempt to Block Bad Ads is Hurting Legitimate Small Business Owners — and its 'Pay-to-Play' Customer Support is Leaving Them Stranded Ahead of the Holiday Shopping Season,* Business Insider (November 25, 2020), https://www.businessinsider.com/facebook-ad-purge-hurting-small-business-owners-holiday-shopping-season-2020-11.

[139] Walt Mossberg, *Mossberg: Lousy Ads Are Ruining the Online Experience,* Vox (January 18, 2017), https://www.vox.com/2017/1/18/14304572/mossberg-lousy-ads.

3. Escalating Data Advantages And Barriers To Entry Fuel Even More Data Extraction

Surveillance advertising giants' data extraction practices ultimately lead to a level of dominance and ubiquity that is both inherently and cyclically anticompetitive, enabling even further unfair practices and cascading data advantages. By originally enticing users with 'free' high-quality products, the dominant platforms are able to collect user data. They then build this data advantage over time by engaging in anticompetitive practices, including data integration across business lines and exclusive dealing.

Once users, publishers, and advertisers are locked into their products -- and the dominant firms are freed from the constraints of competition -- companies like Facebook, Google, and Amazon are free to accelerate their data extraction and monetization practice. They eviscerate privacy protections to build increasingly exhaustive profiles on people, which enables them to deliver hyper-personalized content to each user that's designed to keep them clicking. The unparalleled capacity to precisely target content to a captive user base makes these platforms richer venues for advertisers, thus allowing them to serve more ads and collect more data—which further entrenches their market power. As Sen. Amy Klobuchar (D-MN) recently noted, surveillance advertising creates a huge "barrier to entry when these dominant platforms are able to basically target ads in a way that no one else does because they have all the data… [and] it allows them to create certain algorithms because they have data that no one else has."[140] The fundamental unfair advantage from this business model breaks the supposition of competitive markets by erecting artificial and insuperable barriers.

[140] Margaret Harding McGill, *Senate eyes tech firms' data troves*, Axios (Sep. 21, 2021) https://www.yahoo.com/now/senate-eyes-tech-firms-data-090019271.html.

B. Integration of Data Across Business Lines

The monopoly power of dominant surveillance advertising firms—rooted in the vast troves of data extracted through their platforms—is further entrenched by the *integration* of that data across business lines. As previously discussed, these firms leverage their initial success to establish a broad suite of surveillance points throughout the digital economy. By unifying these private data streams to build increasingly comprehensive user profiles and commercial intelligence hubs, their various business lines gain mutually reinforcing unfair advantages across markets.

Like each of the anticompetitive elements endemic to surveillance advertising, this data integration fuels market distortions that are cyclical in nature. With each additional integrated line of business, the anticompetitive gravity of the surveillance advertising operation as a whole increases; the dominant firms are able to target more ads, with greater precision, across more properties, with fewer constraints, capturing even more data and market power. Thus, at each turn, their ability and incentive to propagate these harms grows; consumers become increasingly unable to escape ubiquitous surveillance ecosystems, and potential rivals face increasingly insurmountable barriers to entry.

Data integration has played a central role in the anticompetitive growth of today's surveillance advertising giants. Facebook, Google, and Amazon have all gained access to a wealth of user data across an ever-expanding constellation of products, services, and third-party mechanisms. Both Facebook and Google have repeatedly misrepresented their intentions, breaking down data silos only after consolidating power in the pertinent markets, while Amazon has spent years quietly positioning itself to exploit its integrated data profiles to fuel its now-exploding surveillance advertising business.

1. Google's Cross-Platform Data Integration

Google became the world's largest search engine in 2000,[141] and has consistently maintained an 80-90% share of the entire U.S. search market for more than a decade.[142] This alone would amount to a massive data advantage over rivals—but that's just the tip of the iceberg when it comes to the company's inconceivable suite of digital surveillance platforms. Beyond its long-standing search monopoly, Google collects and integrates data across major business lines in mobile operating systems (Android), navigation (Maps and Waze), web browsers (Chrome), video streaming (YouTube), app stores (Google Play), email (Gmail), productivity tools (Google Workspace), wearables (Fitbit), smart home devices (Nest), file storage (Google Drive), photo sharing (Google Photos), and more. At least nine of those platforms now have more than one billion users. The data streams from these consumer-facing products are layered on top of, and filtered into, the open display ad tech stack that Google has monopolized.[143]

For many years, as Google built its empire and gained footholds in a slew of digital markets, users could take comfort in the fact that the company kept the personal data they generated on distinct Google-owned properties and services largely compartmentalized. Those long-standing firewalls were eliminated in 2012 in service of the company's surveillance advertising business, as Google merged that data across dozens of services into unified superprofiles for ad targeting, inflicting significant harms to competition across digital markets, and on locked-in consumers and business users who had little choice but to comply. The move drew widespread consternation and transatlantic regulatory scrutiny. In a Gizmodo article entitled,

---

[141] *Google Launches World's Largest Search Engine,* Google News Announcement (June 26, 2000), https://googlepress.blogspot.com/2000/06/google-launches-worlds-largest-search.html.
[142] *Desktop & Mobile Search Engine Market Share United States of America,* StatCounter Global Stats (August 2021), https://gs.statcounter.com/search-engine-market-share/desktop-mobile/united-states-of-america/#monthly-201009-202009.
[143] Harry McCracken, *How Google Photos Joined the Billion-user Club,* Fast Company (July 24, 2019), https://www.fastcompany.com/90380618/how-google-photos-joined-the-billion-user-club.

"Google's Broken Promise: The End of 'Don't Be Evil'," Mat Honan—now the editor-in-chief of MIT Technology Review—explained:

> "Google changed the rules that it defined itself. Google built its reputation, and its multi-billion-dollar business, on the promise of its 'don't be evil' philosophy. That's been largely interpreted as meaning that Google will always put its users first, an interpretation that Google has cultivated and encouraged. Google has built a very lucrative company on the reputation of user respect. It has made billions of dollars in that effort to get us all under its feel-good tent. And now it's pulling the stakes out, collapsing it. It gives you a few weeks to pull your data out, using its data-liberation service, but if you want to use Google services, you have to agree to these rules."[144]

A bipartisan group of 36 state Attorneys General similarly lambasted Google for summarily subjecting business users and consumers to a vast integration of sensitive data across a wide swath of products with minimal ability to opt out and prohibitively high switching costs. The AGs expressed particular concern for Android users, who comprised nearly half the national smartphone market, noting that the "invasion of privacy is virtually impossible to escape" for those consumers, many of whom "no doubt…bought an Android-powered phone in reliance on Google's existing privacy policy, which touted to these consumers that 'We will not reduce your rights under this Privacy Policy without your explicit consent.'"[145]

The Chair of the FTC at the time slammed Google's consolidation of data for presenting consumers with a "binary and somewhat brutal choice."[146] Concurrent investigations were launched by data protection agencies across the UK, France, Italy, Germany, Spain, and the Netherlands,[147] with the Dutch DPA succinctly concluding the "combining of data by Google from and about multiple services and third-party websites for the purpose of displaying personalised

---

[144] Mat Honan, *Google's Broken Promise: The End of 'Don't Be Evil',* Gizmodo (January 24, 2012), https://gizmodo.com/googles-broken-promise-the-end-of-dont-be-evil-5878987.
[145] National Association of Attorneys General, *Letter to Larry Page,* (February 2012), https://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf
[146] Jegg Blagdon, *A 'Brutal Choice': The FTC's Chairman Discusses Google's New Privacy Policy,* The Verge (February 28, 2012), https://www.theverge.com/2012/2/28/2830216/ftc-chairman-google-brutal.
[147] Aaron Souppouris, *Google Braces for Fines in Europe Over Privacy Policy,* The Verge (April 2, 2013), https://www.theverge.com/2013/4/2/4173652/eu-google-privacy-policy-cnil-investigation-conclusion.

ads, personalisation of services, product development and analytics constitutes a major intrusion into the privacy of the users involved."[148]

One of the few Google-owned services that had not been included in the corporation's 2012 unification of personal data was DoubleClick, its ad-serving tool with a massive cache of web-browsing data. As previously discussed, this was part of a long-standing promise. In fact, when Google was in the process of acquiring DoubleClick in 2007, executives made explicit representations to both the FTC and Congress that it could not and would not combine DoubleClick's user browsing data with personally identifiable information from the Google ecosystem. But in 2016, they did exactly that.[149] The move was not just another egregious erosion of consumers' privacy who could no longer escape their ecosystem, but also paved the way for further abuses of power at the expense of publishers, advertisers, and rivals.

Rep. Val Demings (D-FL) grilled CEO Sundar Pichai over this bait-and-switch during the House Antitrust Subcommittee's investigation, noting that when the acquisition was proposed and "alarm bells were raised [about Google's] ability to connect to users' personal identity with their browsing activity," the company assured lawmakers and regulators that wouldn't happen, "but in June of 2016, Google went ahead and merged its data anyway, effectively destroying anonymity on the internet."[150]

Google's integration of extracted data across dozens of touchpoints and third-party sources—sprung upon locked-in consumers and businesses that had no choice but to comply—has been central to entrenching its dominant position across digital markets and raising even greater

---

[148] *Investigation into the combining of personal data by Google*, Dutch Data Protection Authority (November 2013), https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf

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

[150] Supra note 3 at 210.

barriers to entry in online advertising. Oracle Corporation aptly summarized these dynamics in their submission to the Australian Competition and Consumer Commission (ACCC)'s Digital Advertising Services Inquiry:

> "As a result of Google's substantial market power in a number of markets, Google is able to collect vast amounts of data about [users] and to combine it into superprofiles providing Google with intimate and detailed profiles of [their] lives, interests and whereabouts… Those superprofiles allow Google to engage in unrivalled ad targeting. Google's data collection and combination practices, enabled by its Privacy Policy and Terms of Service, create a data moat that constitutes a substantial and insurmountable barrier to entry and competition… Consumers effectively have no choice but to agree to Google's unfair data collection practices because, to do otherwise, would virtually exclude a consumer from using the internet. It is the data moat that Google has created, and the consequential barrier to entry and competition, that enables Google to engage in the other anticompetitive practices that are outlined in this submission."[151]

2. Facebook's Cross-Platform Data Integration

Much like Google, the success of Facebook's initial core product alone gave the company a massive data advantage over its rivals long ago—it has dominated the U.S. personal social networking market for a decade, capturing more than 80% of all time spent by users each year since at least 2011.[152] And much like Google, that has not stopped Facebook from leveraging those gains to drastically expand its anticompetitive surveillance and data integration across new business lines and services.

Facebook's ecosystem also includes the second largest personal social networking service in the U.S. (Instagram), the two most popular mobile messaging apps in the world (WhatsApp and

[151] Australian Competition & Consumer Commission, *Oracle Corporation: Submission to the Australian Competition and Consumer Commission's Digital Advertising Services Inquiry*, 25 (May 13, 2020), https://www.accc.gov.au/system/files/Oracle%20%2813%20May%202020%29.pdf.
[152] Complaint, *Federal Trade Comm. v. Facebook Inc,* Case No.: 1:20-cv-03590-JEB at 65 (August 19, 2021), https://s3.documentcloud.org/documents/21045875/facebook-revised-ftc-complaint.pdf.

Facebook Messenger),[153] and a fast-growing virtual reality platform (Oculus).[154] Considered as standalone products, Facebook Blue, Instagram, and Messenger all rank among the six highest-reach mobile apps in the U.S.[155] Additionally, Facebook has recently been expanding its suite of integrated offerings across adjacent data-rich markets, including Facebook Gaming, Facebook Dating, e-commerce tools like Facebook Shops and Marketplace, and through its Portal smart devices. And as previously described, all of these first-party data streams are bolstered by Facebook's ubiquitous tracking presence across third-party websites and apps that are compelled to rely on its plugins and analytics tools.

Despite a 2011 consent decree ostensibly barring Facebook from misrepresenting personal data collection practices and requiring express consent before weakening users' privacy,[156] the company has repeatedly run roughshod over its own promises and merged data across platforms to further enhance its surveillance advertising business.

When Facebook announced its acquisition of privacy-forward messaging titan WhatsApp in February of 2014—which had approximately 450 million users at the time[157]—CEO Mark Zuckerberg vowed, "We are absolutely not going to change plans around WhatsApp and the way it uses user data. WhatsApp is going to operate completely autonomously."[158] Moreover, Facebook twice told the European Commission during its formal review of the merger that they would be

---

153 Statista Research Department, *Most Popular Global Mobile Messaging Apps 2021,* Statista (Sept. 7, 2021), https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/
154 Casey Newton, *Is Facebook Cornering the VR Market,* The Verge (June 16, 2021), https://www.theverge.com/2021/6/16/22537795/is-facebook-cornering-the-vr-market
155 Supra note 3 at 137.
156 Federal Trade Commission, *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission,* (May 9, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.
157 *Facebook to Acquire WhatsApp,* Facebook Newsroom (February 19, 2014), https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/.
158 Jessica Guynn, *Mark Zuckerberg: WhatsApp Worth Even More Than $19 Billion,* Los Angeles Times (February 24, 2014), https://www.latimes.com/business/la-xpm-2014-feb-24-la-fi-tn-mark-zuckerberg-whatsapp-worth-even-more-than-19-billion-20140224-story.html.

unable to match users' accounts between the apps. Two years later—having eclipsed one billion users—WhatsApp announced it would begin sharing sensitive personal information with Facebook's other platforms for ad targeting purposes,[159] giving users just 30 days to consent and no ability to fully opt out.[160] The E.U. fined Facebook €110 million for willfully misleading the Commission, stating that "contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility."[161] The House Antitrust Subcommittee further asserted, based on their review of contemporaneous internal company documents, that "Facebook intended to create this functionality at the time of the transaction."[162]

For Oculus, Facebook's virtual reality subsidiary, the story was much the same. After being acquired in 2014, one of the brand's co-founders assured concerned customers that they would never need to log into Oculus headsets through a Facebook account, and that, "We are not going to track you, flash ads at you, or do anything invasive,"[163] later saying those promises were approved by Facebook.[164] In 2020, Oculus announced that users would be required to start logging in through a Facebook account, allowing the company to collect and integrate personal data across platforms to improve their surveillance advertising. That change was particularly harmful to

---

[159] WhatsApp, *Looking Ahead for WhatsApp,* Blog Post (August 25, 2016), https://blog.whatsapp.com/looking-ahead-for-whats-app.
[160] Samuel Gibbs, *WhatsApp to Give Users' Phone Numbers to Facebook for Targeted Ads,* The Guardian (August 25, 2016), https://www.theguardian.com/technology/2016/aug/25/whatsapp-to-give-users-phone-number-facebook-for-targeted-ads.
[161] European Commission, *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover,* (May 17, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369.
[162] Supra note 3 at 158.
[163] Jared Newman, *7 Promises Oculus Made After Getting Bought by Facebook,* Time (March 26, 2014), https://time.com/38366/here-are-7-promises-oculus-has-made-after-getting-bought-by-facebook/.
[164] Ian Hamilton (@hmltn), Twitter (Aug 18, 2020, 11:28 AM), https://twitter.com/hmltn/status/1295789706383433734.

parents who'd bought Oculus headsets for children too young to use social media, as Facebook confirmed that minors would not be exempt from this requirement, nor from the subsequent data profiling and targeted advertising.[165] Despite near-universal criticism,[166] Facebook—which has been rapidly amassing power in the VR market in recent years[167]—has plowed forward, recently announcing they would also begin testing in-headset hyper-personalized ads to Oculus users.[168] Already, Germany's Federal Cartel Office has launched separate antitrust actions against Facebook for its anticompetitive maneuvers to expand data integration across both WhatsApp[169] and Oculus.[170]

When Facebook is not using its revenue from surveillance advertising to directly acquire companies for their users' data and attention, it buys them for the capacity to collect ever more invasively. For example, in 2013, Facebook acquired the Tel Aviv-based mobile analytics company, Onavo, for a reported $200 million, just three years after the company's founding.[171] Onavo's business featured two parts: a consumer-facing app to help optimize efficiency on mobile devices, and an analytics business for developers to monitor the performance of their apps against

---

[165] Jefferson Graham, *Parents Furious with Facebook Over Oculus Account Change,* USA Today (Sept. 18, 2020), https://www.usatoday.com/story/tech/2020/09/18/oculus-requires-facebook-account-parents-concern-children-privacy/3481459001/.
[166] N. Summers, *The Oculus Community Hates Facebook's Login Policy Switch,* Engadget (August 19, 2020), https://www.engadget.com/oculus-facebook-login-account-policy-backlash-160034955.html.
[167] Casey Newton, *Is Facebook Cornering the VR Market?,* The Verge (June 16, 2021), https://www.theverge.com/2021/6/16/22537795/is-facebook-cornering-the-vr-market.
[168] Oculus, *Testing In-Headset VR Ads,* Oculus Blog (June 16, 2021), https://www.oculus.com/blog/testing-in-headset-vr-ads/.
[169] The Bundeskartellamt, *Bundeskartellamt Prohibits Facebook From Combining User Data From Different Sources*, Press Release (February 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html;jsessionid=376946F0C7147DF9F98A4D5D26CE1D66.1_cid390?nn=3591568.
[170] The Bundeskartellamt, *Bundeskartellamt Examines Linkage Between Oculus and the Facebook Network*, Press Release (December 10, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2020/10_12_2020_Facebook_Oculus.html.
[171] Ingrid Lunden, *Facebook Buys Mobile Data Analytics Company Onavo, Reportedly For Up to $200M…And (Finally?) Gets Its Office In Israel*, Tech Crunch (October 14, 2013), https://techcrunch.com/2013/10/13/facebook-buys-mobile-analytics-company-onavo-and-finally-gets-its-office-in-israel/.

competitors.[172] Upon acquisition, Facebook used Onavo's VPN app to collect data about users' mobile internet activity, which revealed that WhatsApp, a multiplatform messaging app, was processing over twice as many messages per day as compared to Facebook Messenger.[173] In December of 2020, the Australian Competition and Consumer Commission (ACCC) sued Facebook for promoting Onavo as an app to protect users' data, when in reality, it was "collecting and using the very detailed and valuable personal activity data of thousands of Australian consumers for its own commercial purposes."[174]

While Facebook ultimately shut down Onavo after it attracted significant scrutiny and had been booted from Apple's App Store for violating its data-collection policies, the company has continued to pursue new avenues to gain additional access to competitive intelligence unique user datasets to protect its dominant surveillance advertising business. The company's recent acquisitions of both the GIF platform Giphy, and Kustomer—an upstart customer service CRM platform—are already subject to antitrust investigations,[175] each raising concerns about Facebook boosting its own surveillance advertising business and exploiting new insights about rivals.[176]

---

[172] *Id*.
[173] Josh Constine, *Facebook Will Shut Down Its Spyware VPN App Onavo*, Tech Crunch (February 21, 2019), https://techcrunch.com/2019/02/21/facebook-removes-onavo/.
[174] Australian Competition & Consumer Commission, *ACCC alleges Facebook misled consumers when promoting app to 'protect' users' data*, (December 16, 2020), https://www.accc.gov.au/media-release/accc-alleges-facebook-misled-consumers-when-promoting-app-to-protect-users-data.
[175] Foo Yun Chee, *Facebook's Kustomer Deal May Hurt Competition, EU Regulators Say,* Reuters (August 2, 2021), https://www.reuters.com/technology/eu-antitrust-regulators-investigate-facebooks-kustomer-acquisition-2021-08-02/; and Competition and Markets Authority, *Facebook's takeover of Giphy raises competition concerns* (August 21, 2021), https://www.gov.uk/government/news/facebook-s-takeover-of-giphy-raises-competition-concerns.
[176] Sarah Frier, *Facebook Gets Inside Look at Competition's Data with Giphy Buy,* Bloomberg (May 15, 2020), https://www.bloomberg.com/news/articles/2020-05-15/facebook-s-giphy-purchase-will-help-keep-track-of-competitors?sref=aUHU1jme.

3. *Amazon's Cross-Platform Data Integration*

While Amazon has charted a different course—historically generating minimal revenue from ads as Facebook and Google relied almost entirely on then—it has built an unparalleled hub of consumer profiles and competitive insights integrated across business lines and has quietly laid the groundwork for years to harness this for its now-booming surveillance advertising operation.

Beyond the troves of personal information Amazon already had access to through its dominant e-commerce platform, its ecosystem now includes touchpoints that span grocery shopping (Whole Foods), home security (Ring), gaming (Twitch), video (Prime Video and Fire TV), smart speakers and home assistants (Echo and Alexa), tablets (Fire), e-readers (Kindle), wearables (Halo), wifi routers (Eero), and Amazon is aggressively expanding into the health care space, among other things. All the while, Amazon has been filing a host of patents that shed light on its longstanding desire to use this sprawling surveillance apparatus to target advertisements, including based on changes in users' physical or emotional state,[177] content of recorded conversations,[178] accent and perceived ethnic origin[179], and more. As Tech Transparency Project concluded, "These tools give the company extremely precise insights into the commercial, domestic, travel, social, physical, financial, and even emotional lives of its users—and their friends and family. Amazon then sells that information to advertisers in the form of highly targeted ad placements."[180]

---

[177] Jon Brodkin, *Amazon Patents Alexa Tech To Tell If You're Sick, Depressed and Sell YOu Meds,* ArsTechnica (October 11, 2018), https://arstechnica.com/gadgets/2018/10/amazon-patents-alexa-tech-to-tell-if-youre-sick-depressed-and-sell-you-meds/.
[178] *Amazon Patents 'Voice-Sniffing' Algorithms,* BBC News (April 11, 2018), https://www.bbc.com/news/technology-43725708.
[179] Belle Lin, *Amazon's Accent Recognition Technology Could Tell the Government Where You're From,* The Intercept (November 15, 2018), https://theintercept.com/2018/11/15/amazon-echo-voice-recognition-accents-alexa/.
[180] *Amazon's Data Dragnet,* Tech Transparency Project (January 22, 2021), https://www.techtransparencyproject.org/articles/amazons-data-dragnet.

These threats are not just theoretical. As Amazon expands its surveillance advertising business, it is actively encouraging advertisers to exploit more of the personal data the company has extracted and integrated across business lines.[181] In a recent pitch to advertisers, the company states:

> "Amazon is a store, but it's also much more than that. Customers rely on Amazon to browse new products, watch movies, keep up with their shows, listen to podcasts and music, and read their favorite books. These daily interactions translate to billions of first-party metrics that can help advertisers better understand the audiences that are interacting with their brand across the customer journey, both on and off Amazon."[182]

Indeed, Amazon has been hit with significant fines by the E.U.[183] and France[184] for separate violations in service of their surveillance advertising business over the last year. Even more recently, after the company recently began *paying customers* to register their palm prints for frictionless checkout at retail stores, U.S. Senators pointedly asked Amazon if it will use the biometric data for ad targeting.[185] And now, as both corporate gatekeepers and governments take aim at tracking cookies, Amazon is gearing up to launch its own unique identifier by which advertisers and publishers can better surveil and profile users across its many products and services.[186]

---

[181] Shoshana Wodinsky, *Amazon Asks Its Advertisers to Consider Being A Bit More Invasive,* Gizmodo (December 4, 2020), https://gizmodo.com/amazon-asks-its-advertisers-to-consider-being-a-bit-mor-1845812027.
[182] Katherine Vasilopoulos, *Benefits of Leveraging Behavioral Signals in OTT Advertising,* Amazon Advertising Blog Post (December 2, 2020), https://advertising.amazon.com/blog/behavioral-signals-for-ott-advertising.
[183] Todd Spangler, *Amazon Slapped With Record $887 Million Data-Privacy Fine by EU Agency,* Variety (July 30, 2021), https://variety.com/2021/digital/news/amazon-record-privacy-fine-eu-gdpr-1235031320/.
[184] Commission Nationale de l'Informatique et des Liberté, *Cookies: financial penalty of 35 million euros imposed on the company AMAZON EUROPE CORE* (December 10, 2020), https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core.
[185] Taylor Hatmaker, *Lawmakers Ask Amazon What It Plans To Do With Palm Print Biometric Data,* TechCrunch (August 13, 2021), https://techcrunch.com/2021/08/13/amazon-biometric-data-senate-letter/.
[186] Max Willens, *Amid Post-Cookie Confusion, Amazon Plans to Launch An Identifier of Its Own,* Digiday (June 1, 2021), https://digiday.com/marketing/amid-post-cookie-confusion-amazon-explores-launching-an-identifier-of-its-own/.

4. Consumers Can't Escape; Businesses Can't Compete

As dominant surveillance advertising firms leverage their monopoly power across the entire digital economy by extracting and unifying invaluable private data streams from separate business lines, the harms to competition snowball. With each integration, it becomes more implausible for consumers to escape these vast surveillance networks; these dominant firms expand their control of more critical markets, extract and share more personal data across them, and ratchet up switching costs in each. With each integration, the barriers to entry for existing and nascent competitors become more insurmountable, fighting against an ever-growing spiral of data and monetization advantages. With each integration, advertisers and publishers become more dependent on these surveillance advertising firms to reach their own customers. And with each integration, future business lines gain an even greater leg up in their respective markets.

C. Actively Suppressing Competition Via Exclusive Dealing

Finally, the dominant surveillance advertising firms engage in anticompetitive conduct to actively suppress competition and maintain their monopoly power. While the core collection, monetization, and integration of data grants tremendous 21st century advantages to dominant firms, it also creates the ability and incentive for them to engage in age-old forms of harmful exclusive dealing. Surveillance advertising giants ultimately exploit their power not only to forcibly gather and monetize more data, but to prevent others from gaining a foothold.

The markets in which surveillance advertising thrives are prone to tipping and favor the firms with the most scale. The current dominant firms benefited from these scale effects in the first place to gain the power that they currently enjoy and unfairly abuse. To illustrate, when asked to name Google's biggest strength in 2009, the company's former CEO stated, "Scale is the key. We

just have so much scale in terms of the data we can bring to bear."[187] Similarly, a Facebook representative explained in a 2012 document provided to the House Antitrust Subcommittee, "Advertising is a scale thing, it wasn't until we reached 350 million users did we become interesting to big brands."[188] In this framework, the greatest threats to their dominance comes from the prospect of other firms gaining scale that do not feed into the dominant firm's surveillance business model. The most effective way to suppress competition is to deny scale to competitors and to force existing rivals to feed even more data to the dominant surveillance platforms.

Denying scale to rivals occurs through a variety of means, but the unifying theme is an intent to preemptively neutralize competitors that could otherwise threaten their stranglehold on the market. Specifically, the dominant firms engage in exclusionary conduct to freeze out would-be rivals and punish market participants that seek to circumvent their own prevailing systems of surveillance. Often these practices are combined with the deployment of standards-setting new business lines or products, which allow the surveillance platforms to directly destroy other competitive threats to their business model, such as header bidding.

1. Exclusive Dealing

a. Unilateral Conduct

The first way dominant firms exclude rivals is through unilateral conduct. Because surveillance advertising creates a self-reinforcing growth in scale and resources, the dominant firms often gain gatekeeper status in the digital economy. When threatened by other competitors that might challenge their business model, surveillance advertising platforms have shown a willingness to flatly deny rivals access to the essential chokepoints they control.

[187] Complaint, *United States et. al v. Google*, 1:20-cv-03010, 5 (D.C. Cir.. October 20, 2020).
[188] Supra note 3 at 89.

For one example, Facebook has variously denied rivals access to its APIs like Open Graph at critical moments to disrupt their ability to gain scale when it appeared they may challenge its ability to collect and monetize more user data. Facebook's Open Graph was a tool for users to connect their Facebook profiles and friends to other social media apps.[189] In 2013, Facebook started cutting off its user data to competing apps to throw sand in the gears of fast-growing services. Specifically, Facebook refused to authorize users' requests to find friends on Twitter's Vine app.[190] At the time, Vine was rapidly rising in users and, notably, did not engage in surveillance advertising to the extent that Facebook did. The rise of Vine as an alternative for users threatened to disrupt Facebook's continued ability to unfairly monetize user data, especially through Instagram. Twitter ultimately discontinued the Vine app in 2016 because it struggled to expand its user base, in no small part because of Facebook's exclusive dealing. This is but one microcosm of a far wider trend.

Google's recent initiative with its "privacy sandbox" is a good example of the more amorphous ways that dominant firms try to exclude any challenges to their data collection dominance. Branded as a privacy solution, to create a world without cookies, Google has proposed a number of post-cookie solutions, including the Federated Learning of Cohorts protocol, or FLoC. FLoC is a tracking protocol that Google has designed to run in its Chrome browser that works by creating a tracking label based on a user's browsing history for the past week. FLoC then groups users with similar browsing habits and disseminates a group tag attached to that user to each website the user visits through Chrome.[191] The creation of this new standard for tracking, run

[189] Supra note 3 at 148.
[190] Jeff Blagdon, *Facebook has Apparently Blocked Vine's Friend-Finding Feature*, The Verge (January 24, 2013), https://www.theverge.com/2013/1/24/3913082/facebook-has-apparently-blocked-vines-friend-finding-feature.
[191] Bohn, Dieter, *Privacy and Ads in Chrome are about to Become FLoCing Complicated*, The Verge (March 30, 2021), https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing.

through Google's browser, creates substantial advantages for Google and other surveillance advertising platforms that use its business model.

Unlike in the current tracking environment, FLoC IDs would not be assigned to individual users, but rather to groups ("cohorts") of users with shared characteristics. Thus, it is harder to gather insights on individual users unless they are analyzed at scale with many other groups and associated with other online activity. A platform can reverse engineer insights about the underlying users that compose a cohort if they, like Google, can analyze many FLoC IDs together. This architecture fundamentally advantages the largest surveillance advertising companies, especially Google, Facebook, and Amazon, because their scale allows them to easily replicate the precision data of cookies. Over time, those same dominant platforms can build better analysis tools and collect more information about users over time. This further excludes small players from data gathering and makes today's dominant surveillance platforms uniquely positioned to target advertising, entrenching the unfair advantages discussed above into the foreseeable future.

Because of the power over markets that surveillance advertising firms gain through their business model, they are able to exclude rivals both directly, by denying inputs and access, and indirectly, by structuring digital markets to entrench their dominance and tracking superiority at the expense of users and other businesses.

b. Collusion between Dominant Firms

The second way dominant platforms exclude rivals is through colluding with similarly situated firms in order to neutralize competition. Through collusion, surveillance platforms are further enabled to track more user behavior and further tighten their control over the digital advertising landscape.

In October 2020, the Department of Justice filed its complaint accusing Google of entering into tying arrangements with an intent to block rival search engines.[192] The agreements at issue guaranteed the pre-installation of Google search applications on mobile devices and made them impossible to remove, regardless of consumer preference.[193] Other agreements with Apple required Google to be the *de facto* exclusive general search engine on Apple's Safari browser and other search tools.[194]

Specifically, in 2021, Google drastically increased its payment to Apple in order to secure its placement as the default search engine in Safari on both iOS devices and macOS.[195] The payment also secured Google's position as the default search engine on Apple's "Spotlight" searches on Mac and Siri. From this transaction alone, Google further tightened its grasp on over one billion iOS and Mac users' search data and increased its already significant advantage over competing search engines.[196][197] Apple's senior director of global privacy explained that the company used Google as the default search engine, as opposed to the more privacy conscious DuckDuckGo, due to Google's popularity amongst internet users.[198] While Apple noted that its system can still support search engines like DuckDuckGo and Ecosia, users rarely stray from the default setting and, according to DuckDuckGo, device makers "[require] millions or billions of

---

[192] *Id.* at 3.
[193] United States Department of Justice, *Justice Department Sues Google for Violating Antitrust Laws*, Press Release (October 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.
[194] *Id.*
[195] John Moreno, *Google Estimated to be Paying $15 Billion to Remain Default Search Engine on Safari*, Forbes (August 27, 2021), https://www.forbes.com/sites/johanmoreno/2021/08/27/google-estimated-to-be-paying-15-billion-to-remain-default-search-engine-on-safari/?sh=d92f6db669b0.
[196] Brian Dean, *iPhone Users and Sales Stats for 2021*, Backlinko (May 28, 2021), https://backlinko.com/iphone-users.
[197] Romain Dillet, *There are Now 100 Million Macs in Use*, Tech Crunch (October 30, 2018), https://techcrunch.com/2018/10/30/there-are-now-100-million-macs-in-use/.
[198] Chance Miller, *Apple Privacy Exec Talks iOS 14 Changes and Why Google is Still the Default Search Engine on iPhones*, 9 to 5 Mac (January 28, 2021), https://9to5mac.com/2021/01/28/apple-google-default-search-privacy/.

dollars to become a default browser on a device."[199] Indeed, in its complaint against Google, the Justice Department alleged that such payments "raise barriers to entry for rivals -- particularly for small, innovative search companies that cannot afford to pay a multibillion dollar entry fee."[200]

In addition, Google colluded with Facebook to prevent challenges from header bidding via its Jedi Blue agreement.[201] Jedi Blue guaranteed that Facebook would win a fixed percentage of advertising bids on Google's platform in exchange for Facebook's "bowing out of . . . technology that threatened Google's ad display dominance."[202] Accordingly, smaller rivals are prevented from challenging Google's control over ad-stack and thus its visibility into ad data flows. The agreement also provided that Google would "reveal the identity of a specific percentage of consumers to Facebook, which would help Facebook win more auctions" because advertisers "generally only bid when they recognize the identity of a consumer."[203]

2. *Increasing Surveillance and Market Power by Coercing and Manipulating Market Participants*

In addition to exclusive dealing, dominant surveillance platforms have consistently engaged in the coercion and manipulation of market participants in order to increase their grip over user behaviors. Specifically, firms like Facebook and Google have used various mechanisms to embed their code or integrate tools on publishers' apps and websites in order to surveil and extract third-party data from users as they navigate the digital world. This includes social widgets, logins, pixels, and analytics tools, tying products, and more.

---

[199] Supra note 3 at 181-82.
[200] Supra note at 183.
[201] Mike Swift and Michael Acton, *Google's Description of 'Jedi Blue' Clarifies States' US Antitrust Complaint,* mLex (April 9, 2021), https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/antitrust/googles-description-of-jedi-blue-clarifies-states-us-antitrust-complaint.
[202] *Id.*
[203] *Id.*

While these corporations were once constrained by competitive markets and limited their use of these tools for fear of backlash from consumers and businesses, they have been brazen about exploiting them since consolidating power. Both Facebook and Google have effectively compelled other market participants to change their own privacy policies to cede their own audience data and subject their own users to surveillance advertising giants' tracking and profiling. Specifically, Facebook initially marketed their conversion tracking pixels as "pieces of code" for developers and retailers to "optimize and build audiences for [their] ad campaigns,"[204] however after reeling in enough participants, Facebook "required all businesses to change their own privacy policies to extract from their own users the consent to have Facebook track them for commercial purposes."[205] Google has similarly strong-armed businesses, according to one publisher's description:

> "In the lead up to the commencement of GDPR at the end of May, Google released its updated online terms and conditions, which included changes to its advertising services. The terms were imposed in a non-negotiable way, positioning Google as a co-controller of data for its advertising products, DFP and AdX, and requiring publishers to gain users' consent on Google's behalf to gather and utilise their data."[206]

Dominant firms have also increasingly relied on tying products and services to further their data collection efforts and entrench their dominance in digital advertising. For example, Facebook has successfully gained cross-platform data through tying its login across products including Instagram, WhatsApp, Oculus, and even products not owned by Facebook like Spotify, which users are then unable to disconnect.[207] Additionally, the antitrust suit filed against Google by the Texas Attorney General on behalf of a coalition of ten states accused the company of unlawful tying, citing a series of anticompetitive arrangements that bundled its publisher ad server with its

---

[204] The Facebook Pixel, Facebook for Business, https://www.facebook.com/business/learn/facebook-ads-pixel (last visited Sept. 22, 2021).
[205] Supra note 54 at 73.
[206] The Cairncross Review, *A Sustainable Future for Journalism,* (Feb. 12, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf.
[207] Supra note 3 at 146.

ad exchange, ad network, and ad buying tools, which the complaint calls a significant barrier to entry and expansion in the ad server market.

The Texas suit documents numerous ways in which Google has leveraged its illegal monopoly position to effectively force participants on all sides of the open display market to use its ad tech tools, including paying Google's exchange fees and ad server license fees. Google further entrenches its dominance by using extracted user data to optimize ad bidding strategies with its DSPs—Google Ads and DV360—and has blocked publishers' access to user IDs and charged them additional financial penalties when they trade on non-Google exchanges.

Ultimately, by leveraging its products, Google was able to replace an open header bidding field with its own products and prevent the dilution of its market power. Google's tying of its products effectively destroyed competition in the ad header bidding market. Tying has been a core component of anticompetitive monopoly power in each historical example of monopoly, and it remains a major tool for tech platforms like Google. Given the overwhelming market power maintained by Facebook and Google, and their disproportionate impact on publishers' website traffic and distribution, publishers are left with no choice but to accept these non-negotiable terms despite the significant competitive harms they have and continue to suffer by complying.

Through exclusive dealing and other anticompetitive conduct, dominant platforms have expanded and maintained their monopolies, further enabling them to continue their surveillance over businesses and consumers who are now left without alternatives.

V. THE FTC SHOULD PROHIBIT SURVEILLANCE ADVERTISING AS AN UNFAIR METHOD OF COMPETITION

A. The nature of this business model must be banned entirely.

1. Practices are all integrated

The harms to competition and consumers from surveillance advertising cannot be separated from the business model that produces them. Everywhere it is employed, the surveillance advertising business model unfairly extracts data from users in ways that users would not otherwise accept; it monetizes user data—including from unwilling users or non-users—in ways that unfairly subsidize and entrench the surveillance advertising businesses; it cross-leverages that data to create unfair dominance in other markets, further expanding its practice across the economy; and it relies on anticompetitive and exclusive dealing to prevent the emergence and success of non-surveillance competitors.

2. Harms are integrated

The current giants that employ this model demonstrate the extent to which this conduct is integrated, and that businesses that engage in some portion of these practices ultimately engage in all of them as they gain market dominance. Further, the harms that proceed from this business model are inextricably linked. The increasing collection of personal data erodes the privacy of users and non-users alike, and effectively increases prices. It allows the surveillance advertising giants to target ads in harmful ways, grants them unfair streams of monetization, and entrenches their algorithmic sophistication and dominance. With their troves of data, dominant surveillance advertising firms gain the ability and incentive to consolidate other market segments by cross-leveraging their data and monetization advantages. These factors place rival businesses on a fundamentally uneven playing field, undermining competition across the economy, including in critical ad-supported fields like journalism. Finally, with the monopoly power that comes from

these practices, surveillance advertising platforms engage in exclusive dealing and anticompetitive acquisitions as additional armor against even nascent threats to their exploitative business model.

3. Litigation and other enforcement is ineffective at deterring/solving the harm

Despite the obvious unfairness of the business model, litigation and other enforcement have proven ineffective at constraining its harms. Enforcers have reached substantial settlements and consent decrees with the dominant surveillance advertising platforms in the past.[208] There are several current cases against these same platforms that deal with other aspects of the harm enabled by their business model.[209] Private suits have similarly sought to relieve the injuries caused by these surveillance advertisers for years. These actions have, even where successful, failed to resolve the underlying driver of the harms. Ultimately, litigation and regulatory actions on specific sub-elements of this business model are, by their nature, too slow and too narrowly focused to prevent the effects of an unfair method of competition like surveillance advertising. Without a rule to bar the practice, enforcement and regulatory actions will simply continue to set up dominoes of harm for the next dominant surveillance advertising firm to knock down.

---

[208] Federal Trade Commission, *FTC Approves Final Settlement with Facebook*, Press Release (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Press Release (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, Press Release (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; Federal Trade Commission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, Press Release (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[209] Complaint, *Federal Trade Comm. v. Facebook Inc,* Case No.: 1:20-cv-03590-JEB at 65 (August 19, 2021), https://s3.documentcloud.org/documents/21045875/facebook-revised-ftc-complaint.pdf; Amended Complaint, State of Texas et al. v. Google LLC, 4:20-cv-00957-SDJ, 69 (E.D. Tex. March 15, 2021); Complaint, *United States et. al v. Google*, 1:20-cv-03010, 5 (D.C. Cir.. October 20, 2020); *State of Texas, et al. v. Google LLC,* Case No. 4:20-CV-957-SDJ at 12 (E.D. Tex. December 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216%20COMPLAINT_REDACTED.pdf.

4. Most effective and administrable solution is blanket ban

The most effective, efficient, and administrable solution to these problems is a full ban on the surveillance advertising business model as an unfair method of competition.

The nature of the ban depends on the scope of what conduct is prohibited. It must be broad enough to prevent the suite of harms and market abuses discussed above but narrow and clear enough to be administrable. Further, any rule should make clear that it does not ban all advertising or even all targeting of advertising. This call for rulemaking is not designed to disrupt the ability of publishers and content creators to generate revenue on their sites. For example, search advertising, whereby sponsored ads are provided in response to relevant user queries, and 'contextual' display advertising, whereby ads are targeted based on website, app, or webpage content—similar to most traditional advertising—would remain legitimate. Surveillance advertising consists of two major elements: 1) an information or communication platform collecting personal data and 2) targeting advertisements at users, based on that personal data, as they traverse the internet, including other digital platforms.

The strongest and simplest remedy is to issue a rule prohibiting online platforms from using personal data for the purpose of delivering advertisements.[210] Several such proposals have been made before various lawmaking and regulatory bodies in recent years and the language from those proposals could serve as inspiration for a rule in this context.[211] Such a rule would bar providers of

[210] Personal data includes all data linked or reasonably linkable to an individual or connected device, or group of individuals or connected devices, including inferred and derived data, contents of communications, internet browsing history, and advertising identifiers.

[211] For examples of other proposed language for a blanket ban on surveillance advertising *See, e.g, DSA Proposed Amendment 295* https://www.europarl.europa.eu/doceo/document/LIBE-AM-693830_EN.pdf (Article 2 a Targeting of digital advertising 1. Providers of information society services shall not collect or process personal data as defined by Regulation (EU) 2016/679 for the purpose of determining the recipients to whom advertisements are displayed. 2. This provision shall not prevent information society services from determining the recipients to whom advertisements are displayed on the basis of contextual information such as keywords, the language setting communicated by the device of the recipient or the geographical region of the recipients to whom an advertisement is displayed. 3. The use of the contextual information referred to in paragraph2 shall only be permissible if it does not

digital information and communication services from collecting or processing personal data for the purpose of determining to whom advertisements will be displayed. This formulation of a rule

allow for the direct or, by means of combining it with other information, indirect identification of one or more natural persons, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or persons.);
see also DSA Proposed Amendment 430 *https://www.europarl.europa.eu/doceo/document/LIBE-AM-693830_EN.pdf* (1. Providers of intermediary services shall not collect or process personal data as defined by Regulation (EU) 2016/679 for the purpose of showing digital advertising. 2. This provision shall not prevent intermediary services from displaying targeted digital advertising based on contextual information such as keywords, the language setting communicated by the device of the recipient or the digital location where the advertisement is displayed. 3. The use of the contextual information referred to in paragraph 2 shall only be permissible if it does not allow for the direct or, by means of combining it with other information, indirect identification of a natural person or a clearly identifiable group of recipients/persons, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.);
see also LIBE Committee on Civil Liberties, Justice and Home Affairs of the European Parliament DSA Amendment 58 *https://www.europarl.europa.eu/doceo/document/LIBE-AM-693830_EN.pdf* (1. Providers of information society services shall not collect or process personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679 for the purpose of targeting the recipients to whom advertisements are displayed. 2. By way of derogation from paragraph 1, for the purpose of targeting the recipients to whom advertisements for commercial purposes are displayed, providers of information society services may only collect and use the personal data of recipients who have given their consent as defined in Article 4, point (11), of Regulation (EU) 2016/679 explicitly to such collection and use. Refusing consent shall be no more difficult or time-consuming to the recipient than giving consent. Providers shall not use a method that is designed with the purpose or has the effect of subverting or impairing a recipient's free decision on whether to consent. Recipients whose terminal equipment signals that they object to the processing of personal data when using information society services pursuant to Article 21(5) of Regulation (EU) 2016/679 shall not be asked for consent. 3. Where access to a service requires consent as referred to in paragraph 2 and a recipient has refused to give such consent, the recipient shall be given other fair and reasonable options to access the service. 4. The personal data referred to in paragraph 2 shall not be collected or used for the purpose of (a) targeting recipients based on the actual or likely racial or ethnic origin, the political opinions, the religious or philosophical beliefs, the trade union membership, the health, the sex life or the sexual orientation of a recipient, or (b) targeting recipients below the age of 18. 5. This Articles shall not prevent information society services from determining the recipients to whom advertisements are displayed on the basis of contextual information such as the editorial content in which the advertisement is displayed, keywords, or the geographical region of the recipients to whom an advertisement is displayed.)
see also Committee on Industry, Research and Energy of the European Parliament DSA Amendment 349-350 https://www.europarl.europa.eu/doceo/document/ITRE-AM-695033_EN.pdf (1 a. Providers of hosting services shall, by default, not make the recipients of their services subject to advertisement that is based on the processing of personal data as defined in Regulation (EU) 2016/679 to determine the recipient or the recipients to whom the advertisement is displayed. 1 b. Providers of hosting services may give the recipients of their services the option to receive advertisements that are based on the processing of their personal data. For this purpose only such personal data may be processed, which data subjects have directly and actively provided to the hosting service provider and for the specific purpose of receiving personalised advertisements, provided the conditions for consent laid down in Regulation (EU) 2016/679 have been met, in particular Article 4(11) and Article 7.)
see also Committee on the Internal Market and Consumer Protection of the European Parliament DSA Amendment 1019 https://www.europarl.europa.eu/doceo/document/IMCO-AM-695160_EN.pdf (Providers of intermediary services shall not collect or use personal data of a service recipient for the purpose of targeting or tailoring digital advertising. If a service provider legitimately receives information that allows it to make assumptions about the physical, physiological, genetic, mental, economic, cultural or social identity of a user, this information shall not be used for advertising purposes, specifically not for targeting or tailoring of advertising.)

would directly prevent the core harms of user targeting, unfair monetization, and cross-platform data sharing for advertising purposes. It would also indirectly disrupt the unfair power accumulation that emerges from the flywheel effect of a surveillance advertising business model. The blanket ban of both elements of surveillance advertising through such a rule is the most complete way to prevent abuses of such a business model in the future. It would be the clearest and most easily administrable.

Another version of the rule would address the second element of surveillance advertising: the sharing or use of personal data to target advertisements at users as they traverse the internet.[212] This more restrained rule would prohibit businesses from sharing user data, for the purposes of advertising, to any business line, website, advertising technology, or tracker other than the business or service with which a user intentionally interacts. Moreover, as has been proposed in other contexts, it would simply ban any platform past a certain threshold of users or revenue from using personal data for targeted ads.[213] Thus, a website could advertise directly to its users based on the

---

[212] For examples of similar language that has been considered, see Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) Chapter III https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0842&from=en

(In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall: (a) refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679.);

see also rule language based on the definition of "cross-context behavioral advertising" from the California Privacy Rights Act https://thecpra.org/#1798.140(k) ("Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.")

[213] *See, e.g.*, definitions of "covered platform" in Social Media DATA Act, H.R.3451, 117th Cong. (2021), (https://www.congress.gov/bill/117th-congress/house-bill/3451?q=%7B%22search%22%3A%5B%22%5C%22Social+Media+DATA+Act%5C%22%22%5D%7D&s=2&r=1); *see also* American Choice and Innovation Online Act, H.R. 3816, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3816; Ending Platform Monopolies Act, H.R. 3825, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3825; Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3826; Merger Filing Fee Modernization Act of 2021, H.R. 3843, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3843; ACCESS Act of 2021, H.R. 3849, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3849.

data from interactions on the site, but a digital platform could not combine user data from its email service and smart watch – or from either touchpoint and its ad exchange – for the purposes of targeting ads. While this would not prevent the collection of personal data, it would drastically limit the concentration of that data from multitudinous data collection points into invasive dossiers of information on users.

Such a rule would curb the ability to cross leverage data and advertise to users of a website based on a search they had done earlier in the week or a post they had liked on a social media platform that morning. In this way, it would limit the competitive advantage through subsidization and data leveraging that dominant surveillance advertising businesses enjoy over their competitors. Such a formulation of the rule may risk continuing user and competitive harm from data collection practices, but has the benefit of still preserving a source of revenue for smaller publishers, so long as they do not expand their advertising and data collection beyond the boundaries of their website to create a surveillance apparatus.

Unless the FTC moves to prohibit the surveillance advertising business model at a fundamental level, it will continue to inflict significant and self-perpetuating harms on competition, consumers, and society. We urge the Commission to act expeditiously and use its rulemaking authority to end this unfair method of competition.

CONCLUSION

For the reasons set forth above, the Commission should initiate rulemaking to prohibit surveillance advertising as an unfair method of competition.

Respectfully Submitted,

Nicole Gill, Co-founder and Executive Director
Jesse Lehrich, Co-founder and Senior Advisor

Accountable Tech
1101 Connecticut Ave. NW, Suite 450
Washington, DC 20036
info@accountabletech.org