THE RELATIONSHIP BETWEEN PRIVACY AND ANTITRUST

*Maurice E. Stucke**

INTRODUCTION

Enforcers, policymakers, scholars, and the public are increasingly concerned about Google (Alphabet), Apple, Facebook (Meta), and Amazon. The public sentiment is that a few companies, in possessing so much data, possess too much power. Something is amiss.

Ordinarily, we equate monopolies with higher prices. Unlike some pharmaceuticals or local cable monopolies, these data-opolies do not charge consumers exorbitant prices. Most of Google's and Facebook's consumer products are ostensibly "free." Amazon touts how its consumer-first approach benefits us with low prices and superior service. Apple touts its pathbreaking innovation and building "things that make us proud."[1] So, under the conventional antitrust rubric, free or low prices, better quality, and a lot of innovation do not equal monopolization.

Yet, the bipartisan concern in Congress, which many competition officials around the globe share, is that these powerful firms have monopoly power. All need to be held accountable, and new tools are needed to rein them in.

Why the concern? What exactly are the risks that these data-opolies pose to individuals and society? And more fundamentally, what is the relationship between privacy and competition?

These issues are more fully explored in my recent book, *Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy*.[2] This

* Douglas A. Blaze Distinguished Professor of Law, University of Tennessee College of Law.

1 *Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google: Hearing Before the Subcomm. on Antitrust, Com., and Admin. L.*, 116th Cong. 1 (2020) (statement of Tim Cook, Chief Executive Officer, Apple Inc.).

2 MAURICE E. STUCKE, BREAKING AWAY: HOW TO REGAIN CONTROL OVER OUR DATA, PRIVACY, AND AUTONOMY (2022).

Essay recaps the policymakers', enforcers', and scholars' thinking on the relationship between antitrust and privacy.

Currently, the thinking is that improving privacy protection is a necessary, but not sufficient, step to address some of the risks posed by these data-opolies and deter data hoarding, a key source of their power. The policies proposed in Europe, Asia, Australia, and North America as of early 2022 all assume that with more competition, privacy and well-being will be restored.

In looking at the reforms proposed to date, policymakers and scholars have not fully addressed several fundamental issues. One issue is whether more competition will necessarily promote our privacy and well-being. Another issue is the policy implications if personal data is nonrivalrous. This Essay summarizes a few key themes on the looming conflict between privacy and competition law, and why the traditional policy responses—define ownership interests, lower transaction costs, and rely on competition—will not necessarily work.

I. THE THREE STAGES OF PRIVACY/COMPETITION

A. Privacy/Competition 1.0: No Relationship Between the Two

In 2014, the European Data Protection Supervisor organized in Brussels a conference to explore how privacy, antitrust, and consumer protection policies intersect.[3] It was an unusual gathering, with several competition officials befuddled as to why they were even invited. Privacy, at that time, was a foreign concept to their competitive analysis of mergers and restraints. At that time, several myths were propagated about the digital economy, including:

- Privacy laws serve different goals from competition law;
- The tools that competition officials were then using fully addressed all the big data issues;
- Market forces would solve many privacy issues;
- Data-driven online industries were not subject to network effects and have low entry barriers;
- Data has little, if any, competitive significance, since data is ubiquitous, low cost, and widely available, and dominant firms cannot exclude smaller companies' access to key data or use data to gain a competitive advantage;
- Competition officials should not concern themselves with data-driven industries because consumers generally

3 *See European Data Protection Supervisor Report of Workshop on Privacy, Consumers, Competition and Big Data 2 June* (July 11, 2014), https://edps.europa.eu/sites/edp/files/publication/14-07-11_edps_report_workshop_big_data_en.pdf [https://perma.cc/9BKL-HTMQ].

benefit from free goods and services, and competition always comes from surprising sources; and
- Consumers who use these free goods and services do not have any reasonable expectation of privacy.[4]

Because of these myths, the data-opolies were largely left alone by the competition agencies. Although Google, Apple, Facebook, and Amazon acquired hundreds of companies, few of these mergers were investigated, and none were blocked.[5] The risk that these mergers could degrade privacy was not publicly acknowledged.

One example was Facebook's acquisition of WhatsApp. With its privacy-focused approach, WhatsApp was "the clear 'category leader' in mobile messaging."[6] But the startup also threatened to expand its texting app into Facebook's social networking market. WhatsApp's "stellar growth" was fueled by its "distinctively strong user experience and top-grade privacy protection."[7] To thwart WhatsApp's growth and maintain its social network monopoly, Facebook first launched in 2011 its Messenger texting app.[8] But WhatsApp continued growing. By February 2014, less than five years from its launch, "WhatsApp had more than 450 million monthly active users worldwide and was gaining users at a rate of one million per day, placing it 'on a path to connect 1 billion people.'"[9] So, unable to compete with WhatsApp, Facebook purchased the competitive threat for $19 billion.[10] As one Facebook manager noted approvingly of the merger at that time: "[W]orth it. [WhatsApp's] numbers are through the roof, everyone uses them, especially abroad it [sic]. Prevents probably the only company which could have grown into the next FB purely on mobile[.] . . . [1]0% of our market cap is worth that[.]"[11]

In this merger, privacy was an important facet of nonprice competition. Facebook's texting app was, and remains, free. Facebook harvests its users' data to target them with behavioral advertisements.[12] Unlike Facebook, WhatsApp did not sell advertising

4 For more on these myths, see MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016).

5 *See* David McLaughlin, *Tech Giants Used 'Loopholes' to Duck Merger Reviews, FTC Says*, BLOOMBERG (Sept. 15, 2021), https://www.bloomberg.com/news/articles/2021-09-15/tech-giants-used-loopholes-to-duck-merger-reviews-ftc-says [https://perma.cc/S2PW-9WR8].

6 First Amended Complaint for Injunctive Relief and Other Equitable Relief ¶ 114, FTC v. Facebook, Inc., No. 20-cv-03590 (D.D.C. Aug. 19, 2021) [hereinafter FTC Amended Facebook Compl.].

7 *Id.* ¶ 113.

8 *Id.* ¶ 115.

9 *Id.* ¶ 113.

10 *Id.* ¶ 121.

11 *Id.* ¶ 122 (emphasis omitted) (alterations in original).

12 *Id.* ¶ 45.

space or collect a lot of personal data on its mobile app users.[13] WhatsApp charged users a nominal fee and promised not to collect names, emails, addresses, or other contact information from its users' mobile address books or contact lists other than mobile phone numbers.[14]

None of the competition agencies challenged the transaction, but the European Commission published an opinion explaining its rationale.[15] One positive step was that the Commission recognized that "privacy and security" could be an important, nonprice parameter of competition.[16] Nonetheless, the Commission's analysis of the merger was woefully deficient. For example, it cited the differences in Facebook's and WhatsApp's privacy protections as evidence that the two companies were *not* close competitors.[17] The Commission, in its closing statement, repeated that Facebook Messenger and WhatsApp were "not close competitors and that consumers would continue to have a wide choice of alternative consumer communications apps after the transaction."[18] While recognizing that Facebook may start collecting and using data from WhatsApp users, the Commission had a crimped view about Facebook controlling so much data: "Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[19]

The Commission erred in concluding that the concerns of one firm controlling so much data were strictly a privacy issue, not a competition issue. As the FTC later noted, it was precisely WhatsApp's privacy-focused offerings and design and an ad-free subscription model that provided it "an important form of product differentiation" and helped make it "an independent competitive threat in personal social networking."[20]

Nonetheless, antitrust authorities primarily focused on what was quantifiable (i.e., the mergers' likely impact on price and output), and not what was important in the digital economy (such as privacy, the competitive significance of data, and innovation). So, unsurprisingly

13 *See id.* ¶ 127.

14 *See WhatsApp Privacy Policy*, WHATSAPP, https://www.whatsapp.com/legal/updates/privacy-policy/ [https://perma.cc/FQM7-HMUC]; *Commission Competition Merger Brief*, at 2 n.8 (Feb. 2015).

15 Commission Regulation 139/2004, Case COMP/M.7217—Facebook/WhatsApp, 2014 O.J. (L 2985) ¶ 87 [hereinafter EC Facebook/WhatsApp].

16 *Id.* ¶ 87.

17 *See id.* ¶¶ 102, 107.

18 European Commission Press Release IP/14/1088, Mergers: Commission Approves Acquisition of WhatsApp by Facebook (Oct. 3, 2014).

19 EC Facebook/WhatsApp, *supra* note 15, ¶ 164.

20 FTC Amended Facebook Compl., *supra* note 6, ¶ 127.

they presented no obstacle for the data-opolies' acquiring these nascent competitive threats. As Facebook's CEO expressed in 2008, "it is better to buy than compete."[21] And buy they did.[22]

B. Privacy/Competition 2.0: Privacy as an Important Nonprice Parameter of Competition

By the late 2010s, many scholars, policymakers, and competition agencies were debunking these myths about the digital economy.[23] Looking beyond price and output, they saw how personal data was a key source of these data-opolies' power and the multiple risks that this power posed to our wallets, privacy, autonomy, and democracy. In speaking with market participants and collecting data and records from the data-opolies, policymakers and the competition agencies identified how these data-opolies used the same anticompetitive playbook (including the acquisition of nascent competitive threats) to expand their ecosystem and power, while they continued to degrade individuals' privacy.

In a remarkable turnaround, the policymakers and competition agencies increasingly recognized privacy as an important nonprice component of competition. When a data-opoly's business model depends on harvesting and exploiting personal data, its incentives change. It will reduce privacy protections below competitive levels and collect personal data above competitive levels.[24] Consequently, competition agencies and policymakers were increasingly recognizing

---

21 *Id.* ¶ 1 (emphasis omitted).

22 *See* FED. TRADE COMM'N, NON-HSR REPORTED ACQUISITIONS BY SELECT TECHNOLOGY PLATFORMS, 2010–2019 (2021).

23 Some were debunking these myths well before then, arguing, for example, that privacy harms, while historically not important in antitrust analyses, should be. *See, e.g.*, Google/DoubleClick, F.T.C. File No. 071-0170 (2007) (Harbour, Comm'r, dissenting); Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2017), https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis/ [https://perma.cc/9T9L-PLP9]. But they were, at that time, in the minority.

24 *See* SUBCOMM. ON ANTITRUST, COM. & ADMIN. L. OF THE H. COMM. ON THE JUDICIARY, 116TH CONG., MAJORITY STAFF REPORT AND RECOMMENDATIONS: INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 18 (2020) [hereinafter HOUSE REPORT] ("[I]n the absence of adequate privacy guardrails in the United States, the persistent collection and misuse of consumer data is an indicator of market power online" and "[i]n the absence of genuine competitive threats, dominant firms offer fewer privacy protections than they otherwise would, and the quality of these services has deteriorated over time."); *id.* at 51 (noting how the "best evidence of platform market power" is "not prices charged but rather the degree to which platforms have eroded consumer privacy without prompting a response from the market"); *see also* COMPETITION & MARKETS AUTHORITY, ONLINE PLATFORMS AND DIGITAL ADVERTISING: MARKET STUDY FINAL REPORT ¶¶ 2.84, 3.151 (2020) [hereinafter CMA FINAL REPORT]; AUSTRALIAN COMPETITION & CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY: FINAL REPORT 374 (2019) [hereinafter ACCC FINAL REPORT].

that companies can compete on privacy and protecting data.[25] The collection of too much personal data was seen as the equivalent of charging an excessive price.[26] As the U.K. competition agency noted, "The collection and use of personal data by Google and Facebook for personalised advertising, in many cases with no or limited controls available to consumers, is another indication that these platforms do not face a strong enough competitive constraint."[27] Thus, data-opolies exploit their market power by extracting a lot of personal data from consumers.[28]

---

25 *See* ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, DAF/COMP(2020)1, CONSUMER DATA RIGHTS AND COMPETITION—BACKGROUND NOTE BY THE SECRETARIAT ¶¶ 69, 99, 100 (2020) [hereinafter OECD CONSUMER DATA RIGHTS AND COMPETITION]; *see also* DIGITAL COMPETITION EXPERT PANEL, UNLOCKING DIGITAL COMPETITION 49 (2019) [hereinafter FURMAN REPORT] (also known as the Furman Report); ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, DAF/COMP/WD(2020)51, CONSUMER DATA RIGHTS AND COMPETITION—NOTE BY THE UNITED KINGDOM ¶ 25 (2020) (noting how privacy and data protection rights "may constitute an aspect of service quality on which firms can differentiate themselves from their competitors" and a merger's "reduction in privacy protection . . . may . . . be interpreted as a reduction in quality"); ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, DAF/COMP/WD(2020)40, CONSUMER DATA RIGHTS AND COMPETITION—NOTE BY THE EUROPEAN UNION ¶ 51 (2020) ("Market investigations in specific cases, such as *Microsoft /LinkedIn*, have further supported the view that data protection standards can be an important parameter of competition, particularly in markets characterised by zero-price platform services where the undertaking has an incentive to collect as much data as possible in order to better monetise it on the other side of the platform."); CMA FINAL REPORT, *supra* note 24, ¶ 3.158 (noting that privacy can be a parameter of competition among social media platforms); Complaint ¶¶ 7–8, New York v. Facebook, Inc., No. 20-cv-03589 (D.D.C. Dec. 9, 2020) [hereinafter States Facebook Compl.].

26 *See* OECD CONSUMER DATA RIGHTS AND COMPETITION, *supra* note 25, ¶ 100; CMA FINAL REPORT, *supra* note 24, ¶ 11 (noting that "competition problems result in consumers receiving inadequate compensation for their attention and the use of their personal data by online platforms") (emphasis omitted); ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, DAF/COMP(2016)14, BIG DATA: BRINGING COMPETITION POLICY TO THE DIGITAL ERA—BACKGROUND NOTE BY THE SECRETARIAT ¶ 48 (2016) ("[M]arket power may be exerted through non-price dimensions of competition, allowing companies to supply products or services of reduced quality, to impose large amounts of advertising or even to collect, analyse or sell excessive data from consumers."); *Commission Competition Merger Brief*, at 1, 6 (Feb. 2015), (observing if a website, post-merger, "would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product" then this "could be seen as either increasing its price or as degrading the quality of its product").

27 CMA FINAL REPORT, *supra* note 24, ¶ 6.31.

28 *See, e.g.*, Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html [https://perma.cc/P5F2-9H85] (finding that Facebook abused its dominant position by making the use of its social network conditional on its collecting "an almost unlimited amount of any type of user data from third party sources, allocate[ing] these to the users' Facebook accounts and us[ing] them for numerous data processing processes").

In this second stage, the competition agencies began recognizing privacy as a potentially important parameter of competition.[29] Basically, competition and privacy were seen as complementary. With more competition, firms will be more responsive to our privacy interests.

So, in contrast to the first stage (where the agencies allowed hundreds of acquisitions by Google, Apple, Facebook, and Amazon to sail through without scrutiny or material limitations), policymakers and agencies began investigating these mergers. Most notably, the FTC and many states in 2020 challenged Facebook's earlier acquisitions of Instagram and WhatsApp. They alleged how these acquisitions stifled competition and helped Facebook maintain its social network monopoly. They also alleged how these mergers deprived consumers of the choice of "a personal social networking provider that more closely suits their preferences," including "the availability, quality, and variety of data protection privacy options."[30] Without meaningful competition from these nascent competitive threats, Facebook provided "lower levels of service quality on privacy and data protection than it would have to provide in a competitive market."[31]

Although a district court dismissed the FTC's and states' complaints against Facebook, the court did recognize that a loss in

29 *See, e.g.*, Press Release, European Commission, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 [https://perma.cc/SE7R-K6P4] (acknowledging that privacy was a driver of customer choice and "an important parameter of competition" and that companies can compete on the basis of privacy policy "to the extent that consumers see it as a significant factor of quality"); Commission Regulation 139/2004, Case M.8124—Microsoft/LinkedIn, 2016 O.J. (C 8404) ¶ 350 & n.330; Complaint ¶ 167, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020) [hereinafter Google Compl.] (alleging that by "restricting competition in general search services, Google's conduct has harmed consumers by reducing the quality of general search services (including dimensions such as privacy, data protection, and use of consumer data)"); Complaint ¶ 98, Colorado v. Google LLC, No. 20-cv-03715 (D.D.C. Dec. 17, 2020) [hereinafter Colo. Google Compl.] (alleging that "Google collects more personal data about more consumers than it would in a more competitive market as a result of its exclusionary conduct, thereby artificially increasing barriers to expansion and entry"); States Facebook Compl., *supra* note 25, ¶¶ 127, 177 & 180 (alleging Facebook's degradation in privacy protection after acquiring Instagram and WhatsApp).

30 FTC Amended Facebook Compl., *supra* note 6, ¶ 220; States Facebook Compl., *supra* note 25, ¶¶ 177 & 238–41 (alleging how Facebook changed WhatsApp's terms of service and privacy policy and eroded the preacquisition promises it had made, by combining "user data across the services by linking WhatsApp user phone numbers with accounts on Facebook Blue, enabling WhatsApp user data to be used across all Facebook products," so that Facebook Blue users "who had declined to give their phone numbers to Facebook suddenly found their phone numbers connected to their Facebook Blue accounts anyway").

31 FTC Amended Facebook Compl., *supra* note 6, ¶ 221.

privacy would mean that "millions have experienced a rise in the effective price of using Facebook."[32] (The states appealed the court's dismissal of their claims with prejudice.[33] The FTC was allowed to file an amended complaint, which it did, and which the court subsequently did not dismiss.[34])

In the second stage, a consensus among policymakers emerged on, among other things:

- How the features of the digital platform economy (e.g., the importance of scale, network effects, and high entry barriers) can lead to winner-take-most markets;
- How personal data plays a key role in sustaining the data-opolies' power;
- How neither market forces nor self-regulation will likely mitigate the risks posed by these data-opolies; and
- How additional policy measures are needed.

To address the political, social, and economic risks posed by data-opolies, multiple measures were proposed, with a few already enacted by 2021. One correction was a more proactive review of the data-opolies and their acquisitions. Basically, antitrust enforcers needed to up their game. The 2020 House Antitrust Report was as much an indictment on the U.S. antitrust enforcers and courts as the data-opolies. So the United States joined the competition authorities around the world in investigating the data-opolies and bringing multiple antitrust cases.

But even with increased enforcement, antitrust cases, under the current "rule of reason" analysis, take too long, and the relief, if implemented, is often inadequate to ameliorate the harm. So, policymakers, enforcers, and scholars recognized the need to update

32 New York v. Facebook, Inc., No. 20-3589, 2021 WL 2643724, at *8 (D.D.C. June 28, 2021). The states alleged that as a result of Facebook's preventing, through anticompetitive means, the emergence of viable competitors to its monopoly in personal social networking services, millions of their residents "experienced 'reductions in the quality and variety of privacy options and content available to them' in that market." *Id.* (quoting States Facebook Compl., *supra* note 25, ¶ 8). The court agreed that the states properly pleaded an injury to their quasi-sovereign interests in their economic well-being based on the theory that "millions have experienced a rise in the effective price of using Facebook." *Id.*

33 *See* New York v. Facebook, Inc., No. 21-7078 (D.C. Cir. filed July 29, 2021). The United States filed an amicus brief in support of the States, noting how the district court misapplied the Sherman Act in several fundamental ways. *See* Brief of the United States as Amicus Curiae Supporting Plaintiff-Appellants, New York v. Facebook, Inc., No. 21-7078 (D.C. Cir. Jan. 28, 2022). The appeal, as of early 2022, was pending.

34 *See* Fed. Trade Comm'n v. Facebook, Inc., No. 20-3590, 2022 WL 103308, at *13 (D.D.C. Jan. 11, 2022) (recognizing that allegations of Facebook's degradation of privacy and data protection after acquiring WhatsApp can constitute anticompetitive effects).

and strengthen the competition laws. Policymakers are developing ex-ante codes of conduct to better regulate the behavior of these data-opolies, given their superior bargaining position to advertisers, website publishers, app developers, news organizations, and individuals. For example, Europe's proposed Digital Markets Act imposes seven automatic obligations on gatekeepers, eleven additional obligations, subject to the European Commission's specifications, and potentially more obligations that the Commission could impose under its proposed market investigation tool.[35] These obligations seek to deter many of the data-opolies' abuses, such as self-preferencing, using rivals' data to unfairly compete against them, and tying arrangements.

To make it easier for enforcers to review and block acquisitions by the data-opolies, policymakers are proposing legislative changes to the standard for reviewing conglomerate transactions,[36] lessening the agency's burden of proof to challenge horizontal mergers,[37]

35 *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*, COM (2020) 842 final (Dec. 15, 2020) [hereinafter Digital Markets Act], art. 5 (listing automatic obligations); art. 6 (listing potential obligations); art. 10 (describing the market investigation tool).

36 *See* FURMAN REPORT, *supra* note 25, at 93, 96–97; ACCC FINAL REPORT, *supra* note 24, at 30, 105 (recommending amending merger law to incorporate in the agency's assessment (i) "the likelihood that the acquisition would result in the removal from the market of a potential competitor" and (ii) "the nature and significance of assets, including data and technology, being acquired directly or through the body corporate"); Competition and Antitrust Law Enforcement Reform Act of 2021, S. 225, 117th Cong. (2021).

37 *See, e.g.*, Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Cong. (2021) (prohibiting the largest online platforms from engaging in mergers that would eliminate competitors, or potential competitors, or that would serve to enhance or reinforce monopoly power); Competition and Antitrust Law Enforcement Reform Act of 2021, S. 225., 117th Cong. § 2(b)(2) (2021) (revising "the legal standard under section 7 of the Clayton Act to better enable enforcers to arrest the likely anticompetitive effects of harmful mergers in their incipiency, as Congress intended, by clarifying that the potential effects that may justify prohibiting a merger under the Clayton Act include lower quality, reduced choice, reduced innovation, the exclusion of competitors, or increased entry barriers, in addition to increased price to buyers or reduced price to sellers").

invigorating vertical merger law,[38] and lowering the reporting thresholds for premerger review.[39]

Next are structural remedies. In their antitrust cases against Facebook and Google, for example, the federal and state enforcers are requesting structural remedies.[40] One congressional bill, as part of the antitrust reform package, seeks structural separations and "line of business" restrictions to redress the inherent conflicts of interest when the data-opoly vertically integrates and competes against third-party sellers on its platform (like Amazon, for example).[41]

Unlike the first stage, policymakers and enforcers also recognize the need for greater cooperation among privacy, consumer protection, and antitrust agencies and the need for increased cooperation globally.[42]

Although Google's and Facebook's business model differs from Amazon's, which differs from Apple's, all four companies have been accused of using similar tactics to maintain and leverage their

38 HOUSE REPORT, *supra* note 24, at 395–96 (recommending that "Congress explore presumptions involving vertical mergers, such as a presumption that vertical mergers are anticompetitive when either of the merging parties is a dominant firm operating in a concentrated market, or presumptions relating to input foreclosure and customer foreclosure"); Fed. Trade Comm'n, Statement of Chair Lina M. Khan, Commissioner Rohit Chopra, and Commissioner Rebecca Kelly Slaughter on the Withdrawal of the Vertical Merger Guidelines, FTC File No. P810034 (Sept. 15, 2021); Press Release, U.S. Dep't of Justice, Justice Department and Federal Trade Commission Seek to Strengthen Enforcement Against Illegal Mergers: Agencies Launch Joint Public Inquiry Aimed at Modernizing Merger Guidelines to Better Detect and Prevent Anticompetitive Deals (Jan. 18, 2022) (antitrust agencies seeking "input on whether distinctions between horizontal and vertical transactions reflected in the guidelines should be revisited in light of trends in the modern economy.")

39 Digital Markets Act, *supra* note 35, at art. 12; ACCC FINAL REPORT, *supra* note 24, at 10, 109 (recommending that "large digital platforms should each agree to a protocol to notify the ACCC of proposed acquisitions that may impact competition in Australia"); HOUSE REPORT, *supra* note 24, at 388 (recommending that dominant platforms "be required to report *all* transactions and no HSR deadlines would be triggered").

40 *See* Complaint at 51, FTC v. Facebook, Inc., No. 20-cv-03590 (D.D.C. Dec. 9, 2020) [hereinafter FTC Facebook Compl.] (seeking "divestiture of assets, divestiture or reconstruction of businesses (including, but not limited to, Instagram and/or WhatsApp)"); States Facebook Compl., *supra* note 25, at 75; Google Compl., *supra* note 29, at 57; Colo. Google Compl., *supra* note 29, at 77; Complaint at 8, 115, Texas et al. v. Google LLC, No. 20-cv-00957 (E.D. Tex. Dec. 16, 2020).

41 *See* Ending Platform Monopolies Act, H.R. 3825, 117th Cong. § 2(a) (2021). (prohibiting a covered platform "to own, control, or have a beneficial interest in a line of business other than the covered platform that—(1) utilizes the covered platform for the sale or provision of products or services; (2) offers a product or service that the covered platform requires a business user to purchase or utilize as a condition for access to the covered platform, or as a condition for preferred status or placement of a business user's products or services on the covered platform; or (3) gives rise to a conflict of interest").

42 *See* G7, COMPENDIUM OF APPROACHES IN IMPROVING COMPETITION IN DIGITAL MARKETS ¶¶ 1.8, 4.39 (2021).

dominance. So, the cure is more competition. But will more competition promote our privacy? Not necessarily.

II. PRIVACY/COMPETITION 3.0: THE COMING PRIVACY/COMPETITION DIVIDE

Privacy and competition can be complementary. But more competition will not necessarily improve privacy, especially when the competition itself is toxic. Thus, competition and privacy policies can be at odds, as this Part explores.

A. Toxic Competition

As we examine elsewhere, in the digital platform economy, behavioral advertising can skew the platforms', apps', and websites' incentives.[43] The ensuing competition is about us, but not for us. Here firms compete to exploit us in discovering better ways to addict us, degrade our privacy, manipulate our behavior, and capture the surplus. As Facebook's investor and now critic Roger McNamee observed, "[t]he competition for attention across the media and technology spectrum rewards the worst social behavior."[44]

Take, for example, the competition to track our behavior online. One study examined the extent of online tracking on the top one million websites.[45] It found over 81,000 third-party trackers, with Google and Facebook, by far, leading the pack.[46] Many companies track us only on a few websites. Of these 81,000 third-party trackers, only 123 companies were tracking us on more than 10,000 websites.[47] Only four companies—Google, Facebook, Twitter, and AdNexus—had trackers on more than 100,000 websites.[48] And only Google and Facebook tracked us on hundreds of thousands of websites.[49]

So, even if Google and Facebook were broken up, 81,000 rivals would still compete to track us and better profile us for behavioral advertising. We cannot simply rely on competition to improve our privacy. We first have to ensure the right kind of competition—one

43 *See* STUCKE, *supra* note 2; MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE: HOW FREE MARKET MYTHOLOGY TRANSFORMED US FROM CITIZEN KINGS TO MARKET SERVANTS (2020).

44 ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE 91 (2019).

45 Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, PRINCETON UNIV. DEP'T COMPUT. SCI., https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf [https://perma.cc/X2WR-HRWA].

46 *See id.* § 5.1.

47 *See id.*

48 *See id.*

49 *See id.*

that benefits us. That requires, among other things, aligning incentives, so that data is only collected to benefit us, such as when it is objectively reasonable to provide or improve the requested service. For example, a navigation app could only collect our geolocation data to reflect traffic conditions, not to profile us and target us with behavioral ads. To align incentives, we need baseline privacy protections. This includes effectuating data minimization principles that strictly limit the types of personal information that an organization can collect, how the information is collected, how an organization can use the information internally, and whether, and under what narrow conditions, the data can be shared with others. But that leads to the next fundamental question—

B. What Are the Policy Implications if Data Is Nonrivalrous?

Some economists posit that personal data are nonrivalrous. Unlike a rival good, like a stick of gum, which only one person can consume, a nonrivalrous good can be used and enjoyed by multiple persons. When the same data can be used by many firms without reducing its value, the data is nonrivalrous.

Thus, for some, the welfare-optimal solution is that personal data should be used as much as possible (with a price of zero), for maximizing the potential value from these data. So, we see the emergence of "data philanthropy," where companies can share personal data subject to anonymization with nonprofit organizations who "can unlock the power of private data for the public good."[50] Consider all the potential insights and innovations that access to personal data can unlock, such as the medical insights from our Fitbits or other wearables.

One major cost, however, is the collection, cleaning up, and organization of data. But once collected and organized, data can be easily shared with multiple groups who can use the data for multiple different purposes.

Thus, policymakers are now seeking to deter data hoarding and improve data flow. This includes measures to promote multihoming by users, target the data-opolies' use of defaults to entrench market power (such as Google paying Apple billions of dollars (about $15

50 BRICE MCKEEVER ET AL., DATA PHILANTHROPY: UNLOCKING THE POWER OF PRIVATE DATA FOR PUBLIC GOOD 39 (2018).

billion in 2021[51]) to be the default search engine on Safari);[52] reduce users' switching costs by improving data portability[53] and interoperability;[54] and impose, at times, a duty for data-opolies to share data with rivals while safeguarding individuals' privacy interests.[55]

At the same time, policymakers are seeking to improve privacy protections. The consensus among policymakers is that the current notice-and-consent privacy policies have failed. Policymakers differ on what measures must be undertaken. But they recognize that more robust data minimization policies are necessary so that individuals can regain control over their privacy and limit the personal data that firms can initially collect, use, and share.

We can see how competition law's data democratization policies can clash with privacy law's data minimization policies. If we accept

---

51 Johan Moreno, *Google Estimated to Be Paying $15 Billion To Remain Default Search Engine on Safari*, FORBES (Aug. 27, 2021), www.forbes.com/sites/johanmoreno/2021/08/27/google-estimated-to-be-paying-15-billion-to-remain-default-search-engine-on-safari/?sh=50211652669b [https://perma.cc/TY9J-A3DA].

52 *See* Digital Markets Act, *supra* note 35, at art. 6(1)(b) (requiring gatekeepers to allow end users to uninstall any preinstalled software applications (with one technical-related exception)); American Innovation and Choice Online Act, H.R. 3816, 117th Cong. § 2(b)(5) (2021); Google Compl., *supra* note 29, ¶¶ 47, 118, 175, 182.

53 *See, e.g.*, Digital Markets Act, *supra* note 35, at art. 6(1)(h) (requiring a gatekeeper to "provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access"); ACCESS Act of 2021, H.R. 3849, 117th Cong. § 3 (2021) (giving the FTC new authority and enforcement tools to establish procompetitive rules for data portability online).

54 *See, e.g.*, Digital Markets Act, *supra* note 35, at art. 6(1)(c) (requiring a gatekeeper to "allow the installation and effective use of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the core platform services of that gatekeeper"), (f) (requiring a gatekeeper to "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services"); ACCESS Act of 2021, H.R. 3849, 117th Cong. § 4 (2021) (requiring a covered platform to maintain "a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a competing business" user that complies with the standards issued under the act); HOUSE REPORT, *supra* note 24, at 384–87 (recommending that Congress consider measures to promote data interoperability and portability to encourage competition by lowering entry barriers for competitors and switching costs by consumers).

55 Digital Markets Act, *supra* note 35, at art. 6(1)(j) (requiring a gatekeeper to "provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data"); CMA FINAL REPORT, *supra* note 24, ¶ 8.43; HOUSE REPORT, *supra* note 24, at 20, 385–87.

the assumption of data as nonrivalrous, then we might be predisposed to the collection of personal data, and focus instead on "democratizing" the data—circulating and redistributing the data (with sufficient safeguards) to maximize the overall value derived from the data. But if one simultaneously applies stringent "data minimization" policies, friction arises. These policies seek to limit the flow of personal data in the first instance (from the user to the initial collector). This increases the costs for others to access the data, thereby reducing the potential value that could be unlocked from the data. Thus, these policies can potentially hinder Deep Learning[56] and data-driven innovations.

C. How Do We Define Value, and Value for Whom?

Of course, data sharing can increase the value for the recipients. But critical here is asking how do we define value, and value for whom? Suppose, for example, your geolocation data is nonrivalrous. Its value does not diminish if used for multiple non-competing purposes:

- Apple (or Google) can use your smartphone's geolocation data to track your phone in case it is lost.
- Google Maps can use your phone's location for traffic conditions.
- The government can use your geolocation data to track whether you were in contact with someone with Covid-19 or for general surveillance.
- The behavioral advertiser can use your geolocation data to better profile you and influence your consumption.
- And the stalker can use your geolocation data to terrorize you.

Although each of them can derive value from your geolocation data, you would not necessarily benefit from all of these uses. You may derive value from a very limited purpose—for example, to help find your phone or assess current traffic conditions. But you may not derive value from government surveillance. Nor may you want your data used

56 Deep learning "drives many artificial intelligence (AI) applications and services that improve automation, performing analytical and physical tasks without human intervention." *Deep Learning*, IBM (May 1, 2020), https://www.ibm.com/cloud/learn/deep-learning [https://perma.cc/LY69-GYDS]. A subset of machine learning, it "is essentially a neural network with three or more layers" that attempts to simulate the behavior of the human brain by "learning" from large amounts of data. *Id.* This technology "lies behind everyday products and services (such as digital assistants, voice-enabled TV remotes, and credit card fraud detection) as well as emerging technologies (such as self-driving cars)." *Id.*

for creepy behavioral advertising. Nor would anyone want stalkers to access this data.

So even though the government, behavioral advertisers, and stalkers all derive value from your geolocation data, the welfare optimizing solution is not necessarily to share the data with everyone. Nor is the welfare optimizing solution to encourage competition for our data. The fact that personal data is nonrivalrous does not necessarily point to the optimal policy outcome. It does not suggest that data should be priced at zero. Indeed, pricing data at zero can make us worse off.

The fact that data is nonrivalrous does not mean privacy and competition are inherently at odds. Privacy can be an important nonprice component of competition. Competition along this parameter can deliver greater privacy protection (and better privacy technologies). Likewise, privacy policies can promote healthy competition. But at times, privacy and competition will conflict.

Moreover, the data-opolies will use privacy as a justification for their anti-competitive behavior, such as cutting off rivals' access to personal data. One recent example is Google's announcement that its leading browser Chrome will allow users to block third-party cookies.[57] While Google's move may seem privacy-friendly, one Republican Congressman noted that Google is using privacy "as a cudgel to beat down the competition."[58]

One can discount the data-opolies' privacy justifications as pretextual. But, at a broader level, one can see the conflict between privacy protection and competition. If the privacy laws advance a "data minimization" policy, then there will be far less personal data to democratize. The privacy laws will effectively limit the flow of personal data in the first instance (from the user to the initial collector). Market participants will have to expend the cost and time to collect and process the data, which is problematic when this cost exceeds the potential value that could be unlocked from the data. As a result, the privacy law can hinder data philanthropy, the development of machine learning that relies on a significant volume and variety of data, innovation, and competition.

On the other hand, policymakers, in relying too heavily on data-openness policies, will promote an economy where we become the commodity—where the ensuing toxic competition is how to extract even more data about us (but not for us) and increase our addiction to their websites and apps.

---

57 This is explored in greater detail in STUCKE, *supra* note 2.

58 Nancy Scola, *Why the Tech Giants May Suffer Lasting Pain from Their Hill Lashing*, POLITICO (July 30, 2020), https://www.politico.com/news/2020/07/29/big-tech-ceo-hearing-takeaways-387677 [https://perma.cc/S6G7-VGXJ] (quoting Representative Kelly Armstrong of North Dakota).

When privacy's data minimization strategies are in tension with antitrust's data democratization policies, who should decide these trade-offs, and how? Policymakers, as of early 2022, have not addressed these issues. Instead, they approach the issues circuitously, in promoting one lever (privacy or competition) over another. Overreliance on one lever can tilt the balance between privacy and competition, and leave individuals worse off as a result.

What should policymakers do when competition and privacy conflict? Should we encourage the competition over our data when it primarily benefits advertisers by lowering their costs? Here we as a society are confronted with a quantifiable short-term gain (namely the cost-savings to advertisers) with a privacy harm that is often difficult to quantify and whose risks may be less salient and have long-term implications.

Policymakers may claim a win-win—promote both privacy and competition. That is true sometimes but not always. And their choice of policy tools (tools that democratize data in fostering data collection, through multi-homing and interoperability, and subsequent redistribution, through data portability and imposing a duty to deal) can tilt the balance.

Thus, we are currently left with a market failure where the traditional policy responses—define ownership interests, lower transaction costs, and rely on competition—will not necessarily work.

Moreover, when competition and privacy conflict, at least four traps await policymakers: (i) when in doubt, opt for greater competition (rather than increased privacy protection); (ii) when in doubt, opt for greater privacy over competition; (iii) confusing what is measurable (such as the policies' impact on advertising rates and consumer pricing) with what is important (such as the individuals' well-being); and (iv) embracing privacy measures by the data-opolies when they look like tremendous gains for privacy, except when they aren't (such as Google's bundling YouTube with its DSP services, and enabling users of the Chrome browser to block third-party cookies).

CONCLUSION

Policymakers aptly recognize that they need new tools to tackle the myriad risks posed by these data-opolies. But the best anecdote to the Panopticon World is not in regulating data-opolies with more behavioral dictates. Nor will breaking them apart necessarily promote our privacy, autonomy, and well-being. As long as behavioral advertising persists, so too will the toxic competition. The opportunity costs are enormous. Trust in digital markets will continue to decline, as will the potential value from sharing data. To minimize the looming privacy/competition clash, we need to correct and align the privacy,

competition, and consumer protection policies. This requires multiple policy alignments, as *Breaking Away* examines.[59]

The good news is that we can dismantle the Panopticon where almost every aspect of our lives—where we are, with whom we spend our time, how we spend that time, and whether we are in a romantic relationship—is tracked, predicted, and manipulated. We can also harness the value from data to promote an inclusive economy, that protects our autonomy, well-being, and democracy. In short, a nobler form of competition that brings out our best rather than preying on our worst.

59 *See* STUCKE, *supra* note 2.