Untangling Privacy and Competition

Kenneth A. Bamberger[*] *and Ella Corren*[**]

ABSTRACT: This Article argues that competition law, contrary to the hopes of policymakers and scholars that it offers a powerful tool to combat privacy harms, operates as an anti-privacy framework. Far from a means to address widespread surveillance by market-dominant platforms and other data-intensive firms that monetize the collection and analysis of personal information, competition law's analysis systematically privileges corporate interests at the expense of consumer protection.

This analysis proceeds in two parts. First, the Article identifies the specific competition law concerns raised in recent regulatory enforcement actions and private litigation involving Big Tech, as well as leading scholarship, regarding the ways in which large technology firms secure, enhance, and exploit market power through collection and use of personal data. It then provides an analytic framework that identifies circumstances in which competition concerns align with privacy concerns, pointing in the same regulatory and logical direction, and other circumstances in which those two sets of concerns misalign: where remedies for one might harm the other. Our framework untangles these two sets of concerns and reveals that a majority of competition arguments misalign with privacy. In some misalignment scenarios competition concerns are merely orthogonal to those of privacy, but there is every reason to expect that privacy will be harmed rather than promoted. In others, competition and privacy directly conflict, meaning that promoting competition directly degrades privacy.

Second, the Article reveals two fundamental analytic errors that regulators, courts, and commentators make about privacy in a market setting. These

[*] The Rosalinde and Arthur Gilbert Foundation Professor of Law, University of California, Berkeley; Co-Faculty Director, Berkeley Center for Law and Technology.

[**] Assistant Professor of Law, Bar-Ilan University. Our deep appreciation and respect go to Zhudi Huang and Dan Grushkevich for their excellent research. We would like to thank Orla Lynskey, Alicia Solow-Niederman, and Katrina Ligett for their feedback and insights. In addition, we are grateful for useful comments provided by the participants of the 2025 Privacy Law Scholars Conference, the 2025 Tel Aviv Privacy Conference, the 2025 Private Law Consortium Annual Meeting, the 2025 Israel Law and Economics Association Annual Meeting, the Private and Commercial Law Workshop at the Hebrew University, the Law & Technology Workshop at Tel Aviv University, and the Law & Economics Workshop at Tel Aviv University.

errors dictate privacy-destroying outcomes, even in the instances in which privacy and competition concerns do align.

In the first error, regulators adopt a cramped understanding of the right to privacy as either a superficial concept limited to issues like consent, consumer choice, or data security, or as a means to broader economic goals rather than an essential value on its own terms. Thus, they fail to comprehend privacy as freedom from surveillance. In the second error, competition regulators prioritize markets for surveillance over markets for privacy, either through an agnosticism regarding the substance of the market and a resulting choice to promote the more lucrative and thriving market for surveillance; or through a conceptual confusion between surveillance and privacy markets that obscures the surveillance market's privacy harms.

These errors combine, we show, in a harsh outcome: that privacy concerns are credited in competition analysis only when doing so promotes the health and competitiveness of privacy-eviscerating surveillance markets. The resulting regulatory imbalance ultimately reinforces the dominance of surveillance-driven business models at the expense of consumer and civil rights.

This analysis underscores the conclusion that privacy cannot be effectively regulated through the back door of competition. Rather, the market for personal data should be regulated directly, as we do in other contexts plagued by market failures and harmful underlying behaviors.

INTRODUCTION

Technology firms face increased regulatory scrutiny in the United States and Europe as policymakers seek ways to address both the rising market power of dominant platforms like Meta,[1] Google, and Amazon, and the privacy harms resulting from those firms' collection and use of data. Competition/antitrust[2] laws and privacy regulations have traditionally operated independently in service of distinct goals.[3] Yet the perception of

1. In October 2021, Facebook changed its company name to Meta. Mark Zuckerberg, *Founder's Letter, 2021*, META (Oct. 28, 2021), https://about.fb.com/news/2021/10/founders-letter [https://perma.cc/H958-9X2D]. This Article will use the name Facebook only when discussing cases in which Facebook is a named party; otherwise, the Article will refer to the company as Meta.

2. Throughout this Article, we will refer to competition and antitrust approaches collectively as "competition."

3. *See, e.g.*, MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 4 (2016); Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J.F. 647, 653 (2021) [hereinafter Douglas, *The New Antitrust*]; Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right *[Approach]* to Privacy, 80 ANTITRUST L.J. 121, 138–43

competition law as the potential savior of an otherwise underperforming privacy law[4] has spurred growing calls in scholarship,[5] and efforts in regulatory domains,[6] to use one field to pursue the goals of the other.[7]

Despite the distinct goals of each body of law,[8] regulators often treat the competition–privacy relationship simplistically and unproblematically. And although important recent work has pointed to instances revealing the complexity of combining competition and privacy,[9] scholarship has lacked a comprehensive analysis of the contexts in which the principles of competition may not only diverge from those of privacy, but conflict, with destructive consequences.

This Article fills that gap, concluding that the regulatory imbalance between competition analysis and privacy protection ultimately reinforces

---

(2015); James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1146 (2013); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1010–11 (2013); D. Daniel Sokol & Roisin Comerford, *Does Antitrust Have a Role to Play in Regulating Big Data?*, *in* THE CAMBRIDGE HANDBOOK OF ANTITRUST, INTELLECTUAL PROPERTY, AND HIGH TECH 293, 294–95 (Roger D. Blair & D. Daniel Sokol eds., 2017); FED. TRADE COMM'N, FILE NO. 071-0170, STATEMENT OF FEDERAL TRADE COMMISSION CONCERNING GOOGLE/DOUBLECLICK 2 (2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [https://perma.cc/W6DK-4Z4A] (describing the principle that noncompetition factors should be excluded from competition analysis).

4. GIUSEPPE COLANGELO, INT'L CTR. FOR L. & ECON., THE PRIVACY-ANTITRUST CURSE: INSIGHTS FROM GDPR APPLICATION IN EU COMPETITION LAW 9–10 (2023), https://laweconcenter.org/resources/the-privacy-antitrust-curse-insights-from-gdpr-application-in-eu-competition-law [https://perma.cc/MF8Q-SHB7].

5. *See, e.g.*, Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007), https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis [https://perma.cc/62Y2-7E3Z]; Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 1, 25–26 (2020); Douglas, *The New Antitrust*, *supra* note 3, at 654; Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 773 (2010); Maurice E. Stucke & Allen P. Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, THE ANTITRUST SOURCE, Apr. 2015, at 4, https://www.americanbar.org/content/dam/aba/publishing/antitrust-magazine-online/apr15_full_source.pdf [https://perma.cc/Q3M3-FA5C]; Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 64–66 (2019).

6. *See infra* Sections II.A.1 and II.B.1; *see also* Douglas, *The New Antitrust*, *supra* note 3, at 655 ("The FTC, DOJ, and European competition authorities have adopted this integrated view and have applied it in merger cases." (footnotes omitted)); Maurice E. Stucke, *The Relationship Between Privacy and Antitrust*, 97 NOTRE DAME L. REV. REFLECTION 400, 404–05 (2022).

7. Stucke, *supra* note 6, at 400–01; Matthew Sipe, *Covering Prying Eyes with an Invisible Hand: Privacy, Antitrust, and the New Brandeis Movement*, 36 HARV. J.L. & TECH. 359, 360–62 (2023). Indeed, privacy considerations have been gradually seeping into antitrust law, and vice versa. *See, e.g.*, MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE: HOW FREE MARKET MYTHOLOGY TRANSFORMED US FROM CITIZEN KINGS TO MARKET SERVANTS 216–18 (2020); Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1089–90 (2017) (discussing the role of privacy "lock in" for platform market power).

8. *See, e.g.*, Sipe, *supra* note 7, at 360–67; *see also infra* Part I.

9. For notable examples, see Sipe, *supra* note 7, at 360–62; and Douglas, *The New Antitrust*, *supra* note 3, at 654.

the dominance of surveillance-driven business models at the expense of consumer and civil rights. Competition analysis, we argue, ultimately enacts an anti-privacy framework.

The intuition that competition law, with its focus on tackling market power, offers an effective tool to curb data-abusive market practices is a strong one. Technology giants operate on a business model that involves pervasive commercial surveillance that poses an existential threat to personal privacy.[10] They collect massive amounts of personal information and create digital dossiers about users (and nonusers) of their platforms and services, combine them with information from third parties—including data brokers—and analyze them using artificial intelligence ("AI") to make thick predictions about individual behavior.[11] They exercise market power that can be used to reduce consumer choice over the disclosure and use of personal data. And they dominate what Shoshana Zuboff has described as "surveillance," or "behavioral prediction"[12] markets, by which their massive trove of personal information is monetized through behavioral advertising, or services used to constrain personal choices with regards to, among others, employment, credit, insurance, or pricing. As a result, Senator Amy Klobuchar has written in her book on antitrust in the digital age, "[b]igger is not better when it comes to protecting individuals' privacy rights, because without meaningful competition in the technology sector . . . consumers don't have the prospect of seeing much competition among companies' privacy policies either."[13]

Yet, we argue that, far from being a useful tool for curbing widespread privacy harm by market-dominant firms, competition law actually promotes surveillance markets. This argument proceeds in two parts.

In Part I we dissect the arguments raised by regulators, courts, and commentators about competition concerns that are posed by data concentration, and assess their relative alignment with concerns regarding privacy. These arguments fall into two categories. The first involves the concentration of data as a resource or business asset that can lead to market power and create barriers to entry by rivals.[14] The second views privacy as a quality (non-

10. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 10 (2019) ("Surveillance capitalism's products and services . . . are the 'hooks' that lure users into their extractive operations in which our personal experiences are scraped and packaged as the means to others' ends.").

11. *See generally* Samuel Levine, Dir., Bureau Consumer Prot., Fed. Trade Comm'n, Keynote Remarks at the Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference 2–3 (May 19, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf [https://perma.cc/TN9U-2EUA] (describing the elements of "the pervasive and comprehensive tracking of consumers' movements and behaviors across virtually every aspect of our daily lives," and its monetization).

12. ZUBOFF, *supra* note 10, at 8–10, 96.

13. AMY KLOBUCHAR, ANTITRUST: TAKING ON MONOPOLY POWER FROM THE GILDED AGE TO THE DIGITAL AGE 346 (2021).

14. These arguments are discussed below in Section II.A.1.

price) dimension of products or services on which firms might compete, or as a proxy for the actual cash price consumers are paying, on the assumption that they pay with their data.[15] On this view, data concentration can result in a reduction in product quality or increase in consumer price in the form of data extraction and privacy erosion.

In both categories, we explain, many competition arguments misalign with privacy concerns. In the cases where competition law treats data as a business asset and data concentration as a barrier to market entry, most competition arguments are merely orthogonal to those of privacy—yet there are good reasons to believe that measures to reduce concentration might hurt privacy rather than protect it. These measures compel or facilitate data flows among rivals with the aim of increasing competition, but in doing so, they simultaneously erode and marginalize privacy. Moreover, in the largest category of privacy-as-quality cases, competition and privacy directly conflict, as data-protective practices may in and of themselves exclude competitors and reinforce market dominance. In these scenarios, promoting competition is directly intended to degrade privacy protections in the name of dissolving market concentration.

Part I, however, also identifies two important instances in which privacy and competition concerns *do* align. The first involves rare cases in which regulators have used competition proceedings to limit the combination and use of data, mostly during the regulatory review of mergers and acquisitions—a context where data is viewed as a business asset. The second involves the scenario in which, because of the lack of competition over privacy, firms can use their market power to "lock in" consumers to poor or worsening privacy conditions, and thereby lower quality.

Even in those two instances of potential alignment between competition and privacy concerns, there is little reason for optimism. Part II identifies two errors pervasive in regulatory analysis across the range of recent competition cases that lead to a loss for privacy even in those previously identified scenarios in which privacy and competition theoretically align.

The first is an error in defining *privacy* that misapprehends both the economics of privacy and the reality of market data behaviors. Specifically, regulators frame privacy as something external to market dynamics, equate it with surface-level consent, consumer choice, or data security, and treat it as a means to broader economic goals rather than an essential right on its own terms—yet they fail to recognize privacy more broadly as freedom from surveillance. This thin version of privacy competes poorly against other market values in the competition calculus. While our critique of this thin conception of privacy is aimed primarily at competition regulators, it also extends to approaches adopted by privacy regulators and embedded in privacy law more generally. Although developing a full account of privacy as freedom from

15. These arguments are discussed below in Section II.A.2.

surveillance is the subject of a separate article,[16] Part II demonstrates how, in the context of "the market," a too-thin conception of the right to privacy generates significant shortcomings and problems, and how a collapsed definition of privacy proves unworkable, particularly for controlling market actors.

The second error involves a misguided analysis of *markets*. Regulators conflate consumer markets, where privacy could theoretically be a competitive factor, with surveillance markets, where privacy is either irrelevant or obstructive to competition. Their analysis ignores the reality that, for a variety of reasons, privacy is both: (1) not significantly subject to competition; and (2) harmed by improved surveillance markets.

Together, we show that these errors effectuate an anti-privacy regulatory framework by which competition legitimizes surveillance markets and, even in the limited instances in which privacy and competition values might align, privacy violations will (ironically) only be credited in service of promoting these privacy-destructive markets. Our argument, then, is not only that firms are not competing over privacy, or that firms are not competing enough full stop—we go a step further to argue that it is *unrealistic* to expect firms to compete over privacy when regulatory frameworks support a surveillance economy which is directly antithetical to a market for privacy.

Thus, in Part III, we ultimately argue for untangling the regulatory efforts behind competition and privacy. Competition law's indirect approach fails to protect privacy in the digital age, and the issue of surveillance markets dominated by powerful firms cannot be resolved without direct behavioral regulation limiting the collection, use, and monetization of personal data through surveillance markets. As with other markets afflicted by structural failures and harmful practices, meaningful intervention is necessary to curb exploitation and protect fundamental rights.

I. UNTANGLING COMPETITION AND PRIVACY CONCERNS

In today's surveillance economy, market dominance can arise from the competitive advantage accorded by access to consumer data unavailable to potential competitors, the ability to combine that data with data from other sources like third-party websites and other online tracking, and the resulting ability to surveil consumer activities, grow a database of personal information, and extract information in ways that increase the value of behavioral advertising models over those of rival firms.[17]

16. *See* Kenneth A. Bamberger & Ella Corren, *Privacy as Freedom from Surveillance* (unpublished manuscript) (on file with the Authors).

17. Kyriakos Fountoukakos, Marcel Nuys, Juliana Penz & Peter Rowland, *The German FCO's Decision Against Facebook: A First Step Towards the Creation of Digital House Rules?*, 18 COMPETITION L.J. 55, 58 (2019) (discussing the 2019 decision by the German Federal Cartel Office against Facebook for its abuse of a dominant position through data collection practices, and noting that "as a consequence of Facebook's high user numbers, advertising-financed business models prevail in the market"); STAFF OF H. COMM. ON THE JUDICIARY, SUBCOMM. ON ANTITRUST, COM. & ADMIN.

As regulators and commentators have noted, the resulting market concentration can significantly harm privacy in a number of ways.[18] Market-dominant firms have greater power to collect and utilize user data, leading to increased surveillance and potential misuse of personal information.[19] They have fewer competitive incentives to engage in strong privacy protections.[20] They can also use their market power to exclude or disadvantage third parties,[21] including those engaged in privacy-protective practices.[22] Moreover, mergers with, or acquisitions of, smaller data-intensive market players have enabled firms to expand and deepen their capabilities to collect and analyze personal data.[23]

A significant September 2024 Federal Trade Commission ("FTC") report[24] makes the connection between market concentration and privacy concerns explicit. It points to the "dominant positioning enjoyed by the largest firms, which exert vast power over our economy, our democracy, and our society."[25] And it identifies the risk, given market incentives to harvest data, that they will use that power to:

L., 117TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REPORT AND RECOMMENDATIONS 33 (Comm. Print 2022), https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf [https://perma.cc/KKN5-W37Y] ("[A] dominant platform can use its market power to extract more data from users, undermining their privacy.").

18. Douglas, *The New Antitrust*, *supra* note 3, at 656 ("Recent characterizations of digital market power and abuse of dominance similarly link the decline of competition with the erosion of data privacy.").

19. Philipp D. Dimakopoulos & Slobodan Sudaric, *Privacy and Platform Competition*, 61 INT'L J. INDUS. ORG. 686, 688 (2018) (deriving models indicating that weak platform market competition will lead to overcollection of private data).

20. *See* Ariel Ezrachi & Maurice E. Stucke, *Distortions: How Data-opolies Are Dissipating the Internet's Potential*, *in* DIGITAL PLATFORMS AND CONCENTRATION 5, 6 (Guy Rolnik ed., 2019), https://www.promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf [https://perma.cc/UF6Q-ZZCG] ("Leading platforms can depress privacy protection below competitive levels and collect personal data above competitive levels.").

21. European Commission Press Release IP/21/3143, Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector (June 21, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143 [https://perma.cc/W25E-GTTR].

22. *See* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 179–85 (2016) (discussing Google's exclusion of privacy app Disconnect from the Android app store).

23. *See Competition and Privacy*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/consumer-privacy/competition-and-privacy [https://perma.cc/JK62-VHZA] (describing that the Electronic Privacy Information Center "has shown the FTC in numerous antitrust and privacy complaints that each acquisition by a dominant firm has led to a reduction in both competition and privacy protection," and providing links).

24. *See generally* FTC, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES (2024) [hereinafter FTC SOCIAL MEDIA REPORT], https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services [https://perma.cc/KP7N-QMUK].

25. *Id.* at ii.

> seek unfair advantages through a host of anticompetitive behaviors – from pressuring smaller websites to embed their tracking technologies, to leveraging their massive collection efforts to identify and prevent newcomers who want to enter the market, to creating vast 'walled gardens' that do much to depress competition and little to protect consumers' data.[26]

The link between data concentration by entrenched dominant firms and the erosion of privacy raises the allure that steps to reduce market concentration will enhance privacy (and vice versa). As former FTC Commissioner Rohit Chopra has described, "in the digital economy, the data that companies compete to obtain and utilize is also at the center of significant privacy and data security infractions."[27] A celebrated 2021 joint statement by the U.K. Competition and Markets Authority and Information Commissioner's Office explicitly embraced this notion. Rejecting the proposition that "[t]he objectives of competition law and data protection are sometimes characterised as being in opposition," they concluded: "We do not agree."[28] Rather, the regulators jointly asserted that, not only explicit "standards and regulations to protect privacy," but also remedies such as user choice and control and "data-related interventions to promote competition," will further data protection.[29] In the words of former E.U. Competition Commissioner Margrethe Vestager, "if privacy is something that's important to consumers, competition should drive companies to offer better protection."[30]

But untangling actual antitrust concerns about concentrated data markets and comparing them to privacy concerns suggests that this intuition is uncertain at least, and unfounded at most. The relation between market concentration and privacy is far messier.

To be sure, in some cases, competition and privacy regulators have collaborated to identify individual instances in which both concerns are individually implicated, or where the enforcement of one does not undermine the other. Both European competition and data protection authorities,

---

26. *Id.*

27. Statement of Commissioner Rohit Chopra, Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security 5 (June 17, 2020), https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpipchoprastatement.pdf [https://perma.cc/QX3Q-Q9EE].

28. COMPETITION & MKTS. AUTH. & INFO. COMM'R'S OFF., COMPETITION AND DATA PROTECTION IN DIGITAL MARKETS: A JOINT STATEMENT BETWEEN THE CMA AND THE ICO 18 (2021) [hereinafter U.K. REGULATORS JOINT STATEMENT], https://assets.publishing.service.gov.uk/media/60a3c893d3bf7f288aaa5c9b/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf [https://perma.cc/684W-T6ZL].

29. *Id.* at 19.

30. Margrethe Vestager, Comm'r for Competition, Eur. Comm'n, Mackenzie Stuart Lecture at Cambridge: Making the Data Revolution Work for Us (Feb. 4, 2019), https://wayback.archive-it.org/12090/20191129203859/https:/ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-revolution-work-us_en [https://perma.cc/FKV5-QR56].

for example, raised concerns about Apple's proposed 2018 acquisition of Shazam, a competitor streaming service and music identification app. On the competition side, the transaction could have allowed Apple to "obtain access to commercially sensitive data about customers of its competitors," allowing it to "directly target its competitors' customers and encourage them to switch to Apple Music."[31] On the privacy side, such economic concentration implicated data protection and consumer rights concerns.[32] Similarly, a part of the standard for assessing the legitimacy of privacy-intrusive practices under Section 5 of the FTC Act asks whether those practices are "outweighed by countervailing benefits to consumers or competition."[33] Where a firm's behavior devalues privacy with no competitive benefit, enforcement may be conceptually unproblematic.

But the intuition that the link between dominant firms in data-intensive markets and privacy erosion means that decreasing concentration will improve privacy is more complicated.

Untangling the various arguments that regulators, courts, and commentators make against data concentration provides insight into that complexity. This Part distinguishes two ways in which competition arguments about data collection are framed. The first type of argument goes to the competition concerns about concentration of data as a resource or business asset. The second type of argument frames the effects of data concentration directly on outputs, suggesting that this concentration results in a diminishment of privacy that should be understood as a reduction in product quality, or increase in consumer price, in the form of data extraction and privacy erosion.

Examining these two types of arguments exposes different types of regulatory mismatches between competition enforcement priorities and privacy protection, all of which suggest that the aims of competition law do not—or at least do not reliably—align with privacy protection. As the remainder of this

---

31. European Commission Press Release IP/18/3505, Mergers: Commission Opens In-Depth Investigation into Apple's Proposed Acquisition of Shazam (Apr. 22, 2018), http://europa.eu/rapid/press-release_IP-18-3505_en.htm [https://perma.cc/LZ3G-9F9E].

32. Statement of Eur. Data Prot. Bd., Data Protection Impacts of Economic Concentration (Aug. 27, 2018), https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-edpb-data-protection-impacts-economic_en [https://perma.cc/KQ6Z-QU99].

33. *See, e.g.*, Complaint at 11, 1Health.io, No. 1923170 (F.T.C. Sept. 6, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/complaint.pdf [https://perma.cc/8NCC-RLKT] (alleging that "[r]espondent's retroactive application of its revised privacy policies caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition"); Complaint at 19, FTC v. Ring LLC, No. 23-cv-1549 (D.D.C. May 31, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/complaint_ring.pdf [https://perma.cc/82HY-HH6U] (alleging that "allow[ing] thousands of employees and contractors to access video recordings of customers' intimate spaces without customers' knowledge or consent" caused "substantial injury to consumers . . . that is not outweighed by countervailing benefits to consumers or competition"); Complaint at 15–16, United States v. Edmodo, LLC, No. 23-cv-02495 (N.D. Cal. May 22, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/edmodocomplaintfiled.pdf [https://perma.cc/8YG4-UFB5] (alleging that "[d]efendant's attempts to outsource its legally-mandated responsibility for COPPA compliance onto schools and teachers . . . provided no countervailing benefit to consumers or competition").

Part explores, regarding the first category of arguments, reduction of data concentration sometimes promotes privacy interests, but often misaligns with them. Regarding the second, competition concerns about the market power of dominant firms to reduce competition on product quality similarly cuts both ways. Market power might be used to enable firms to erode user privacy (and therefore product quality) by "locking" those users into an inferior product; here, privacy and competition concerns strongly align. Or it might be used by "gatekeepers" in otherwise anticompetitive ways that could, at least in theory, promote privacy; here, privacy and competition concerns misalign.

This examination in turn sets the foundations for the discussion in Part II, which further explores the identified contexts in which competition and privacy concerns align. There we argue that two errors endemic to current competition analysis nonetheless result in a net privacy loss.

A. Competition Concerns over Data as a Business Asset: The Tension Between Reducing Data Concentration and Privacy

1. Alignment Between Competition Approaches and Privacy Concerns: When Reducing Data Concentration and Use Can Reduce Surveillance at the Firm Level

Competition regulators have come together on at least one paradigmatic context in which data concentration might run afoul of both competition and privacy principles: the combination of formerly distinct datasets, for example after a merger or acquisition. As the U.K. competition and privacy regulators together explained, restricting the ability of companies to combine datasets "could in principle deliver strong synergies between the interests of competition and data protection, since they involve restricting the ability to combine and process personal data, at the same time as creating a more level playing field for all businesses to compete fairly."[34]

Accordingly, regulators have, albeit rarely,[35] taken the opportunity of merger reviews to restrict the ability of platforms with market power to combine personal data in ways unanticipated by users. The idea is that when regulators limit data combinations in service of market competition—often defined as

34. U.K. REGULATORS JOINT STATEMENT, *supra* note 28, at 23; *see also* Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES L. 189, 197–200 (2019).

35. *See, e.g.*, Orla Lynskey, *Delivering Data Protection: The Next Chapter*, 21 GER. L.J. 80, 83 (2020) ("[B]etween 2008 and 2018, a facilitating mergers and acquisitions regime has enabled Google to acquire 168 companies; Facebook to acquire 71 companies and Amazon to acquire 60 companies. Whether these mergers constituted 'killer' acquisitions, which had the object or effect of stymying nascent competition was a question for competition law. By consolidating a greater volume and variety of user data in the hands of a small number of unavoidable actors, however, the environmental changes enabled by competition law also have an effect on data protection." (footnote omitted)).

the market for advertising or other behavior predictions—it can also serve the goals of privacy—defined as user control over information.[36]

Three notable cases point to this goal alignment: the European Commission's clearance of Google's 2020 merger with Fitbit, the earlier regulatory approval of Facebook's acquisition of WhatsApp in 2014, and an action brought by the German Competition Authority (the Bundeskartellamt) against Facebook that, after five years of proceedings in different venues, reached resolution in October 2024. These cases will arise again throughout our discussion of the ways that, even in the limited context in which privacy and competition concerns align, errors in competition analysis will largely still result in privacy-corrosive outcomes.[37]

The Google–Fitbit merger was ultimately approved after certain anti-concentration concessions by Google to promote user control over personal data. Specifically, Google committed to "silo" health and wellness data collected from Fitbit wearable devices apart from other Google data used for advertising, and to refrain from using Fitbit-derived data for advertising. This would, in turn, provide users an "effective choice to grant or deny the use of [such] data . . . by other Google services (such as Google Search, Google Maps, Google Assistant, and YouTube)."[38]

Concern about the combination of data had been raised, although was handled more clumsily, in the regulatory approval process for Facebook's acquisition of WhatsApp in 2014. The European Commission, which reviewed the merger, called into question whether Facebook could potentially combine user data across both platforms to gain an unfair competitive advantage in the online advertising market.[39] Ultimately, the European Commission approved the merger without imposing data sharing restrictions, noting in its review that the two companies had indicated, in a variety of ways—representations to the European Commission and to the public, documentation submitted during the review, and shared assumptions about consumer backlash if they would combine data—that they would not, in fact could not, feasibly combine their user datasets because of the distinct technical architectures and user identifiers used by the two platforms.[40]

---

36. The way these definitions predetermine privacy-corrosive outcomes is discussed in Part II below.

37. *See infra* notes 332–37 and accompanying text.

38. European Commission Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 [https://perma.cc/M4MY-AUXV].

39. EUR. COMM'N, CASE NO COMP/M.7217 - FACEBOOK/WHATSAPP ¶¶ 160–61, 184 (Mar. 10, 2014) [hereinafter FACEBOOK/WHATSAPP EC MERGER REVIEW], https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf [https://perma.cc/6QHM-WNQX] (recounting arguments that "integration would allow Facebook to have access to additional data from WhatsApp users to be monetised through advertising").

40. *Id.* ¶¶ 138–39, 160–61, 184–85. In any event, the European Commission concluded that "even if the merged entity were to start collecting and using data from WhatsApp users,"

Although the FTC's Antitrust Bureau did not stop the merger, albeit without providing public details on reasoning or any investigation it conducted, the Commission's Consumer Protection Bureau did send both firms a letter recognizing the importance for privacy of the firms' commitments about data use, reminding them of their "obligations to protect the privacy of their users in light of Facebook's proposed acquisition of WhatsApp."[41] The letter detailed the privacy "promises" WhatsApp provided its users at the time of the merger, including the promise to keep WhatsApp separate from Facebook post-merger and to maintain the same data and privacy practices post-merger.[42] It further cautioned that any deviation could constitute a violation of Section 5 of the FTC Act, or of the FTC order against Facebook at that time.[43]

Finally, concerns about data combination and concentration arose in what commentators have recognized as one of the most promising instances of using competition law to protect privacy: the German Facebook case. In a landmark 2019 decision, the Bundeskartellamt ruled that Facebook had engaged in anticompetitive behavior by abusing its dominant market position through the collection and combination of personal data from its various services and third-party sources without user consent.[44] The agency found that the data combination, which violated privacy law, granted Facebook an unfair advantage in surveillance markets.[45] On appeal, the Court of Justice of the

---

this could not raise competition concerns because of the European Commission's market investigation, which concluded that "post-Transaction, there will remain a sufficient number of alternative providers of online advertising services." *Id.* ¶ 187–89. When it was later revealed that the technical feasibility to match and combine Facebook's and WhatsApp's user databases existed at the time of the merger and that Facebook knowingly misled the regulator, the Commission fined Facebook €110 million, but did not open its previous decision to allow the merger. European Commission Press Release IP/17/1369, Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information About WhatsApp Takeover (May 18, 2017), https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1369 [https://perma.cc/6JUG-5R2P].

41. Press Release, FTC, FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition (Apr. 10, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed-acquisition [https://perma.cc/T9D7-UWED].

42. Letter from Jessica L. Rich, Dir., Bureau of Consumer Prot., to Erin Egan, Chief Priv. Officer, Facebook, Inc. & Anne Hoge, Gen. Couns., WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf [https://perma.cc/89E8-K36M].

43. *See id.* at 3. *But cf.* FTC, *supra* note 3, at 2–3 (considering, but largely dismissing, concerns over the privacy effects of the merging parties combining their respective sets of advertising data).

44. Press Release, Bundeskartellamt, Facebook Proceeding Concluded (Oct. 10, 2024), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html [https://perma.cc/QTH8-HFUJ].

45. *See, e.g.*, Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship Between Competition and Data Protection Law*, 54 EUR. J.L. & ECON. 217, 219 (2022); *see also* Inge Graef, Damian Clifford & Peggy Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law*, 8 INT'L DATA PRIV. L. 200, 210 (2018) (noting the Bundeskartellamt's approach and advocating for "[d]ata protection and consumer law principles as benchmarks for exploitative abuse").

European Union ("CJEU") ruled explicitly that competition authorities can consider violations of privacy law when investigating abuse of a dominance cases.[46] In October 2024, after finally concluding its proceeding, the agency's president heralded "significant changes" in data handling, notably the fact that the platform "no longer requires users to consent to Meta collecting a limitless amount of data and linking such data to their user accounts" as a condition of consumers' use of the platform's services.[47]

These cases illustrate a seemingly straightforward, logical alignment argument between competition and privacy concerns: Restricting the combination of datasets can promote competition by limiting data-driven market power, while simultaneously preserving privacy by preventing cross-analysis and inferences across previously separate datasets.

2. Misalignment Between Competition Approaches and Privacy Concerns: Lowering Data Barriers to Entry and Reducing Concentration in Data Markets Can Harm Privacy

The Google–Fitbit and German Facebook cases offer scenarios in which competition might be promoted by the limitation on data concentration and use within a single firm, an approach that aligns with privacy concerns. Yet the more widespread regulatory approach to addressing the central role that access to data plays in maintaining and extending market dominance—reducing data concentration in an attempt to ensure that rivals are not foreclosed from access to data markets—cuts the other way.[48] This approach, reflected in regulation, enforcement actions, and enhanced scrutiny of mergers with an eye on data concentration, seeks to increase competition by lowering data barriers to market entry.[49] In the words of former European Competition Commissioner Margrethe Vestager, "as data becomes increasingly important for competition, . . . giving access to data" may be "the best way to restore competition."[50] Yet for a variety of reasons, these pro-competition approaches might harm privacy, while concentration might benefit it, illustrating a dynamic where privacy and competition are inversely related.

---

46. Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 48 (July 4, 2023).

47. Press Release, Bundeskartellamt, *supra* note 44.

48. U.K. REGULATORS JOINT STATEMENT, *supra* note 28, at 22 (citing "the need to overcome significant disparities in access to data that have the potential to distort competition").

49. Press Release, FTC, Federal Trade Commission Announces Hearings on Competition and Consumer Protection in the 21st Century 3 (June 20, 2018), https://www.ftc.gov/system/files/attachments/hearings-competition-consumer-protection-21st-century/hearings-announcement_0_0.pdf [https://perma.cc/QQ79-AVBZ] (considering how data sharing could enhance consumer choice and improve competitive dynamics).

50. Margrethe Vestager, Comm'r of Competition, Eur. Comm'n, Speech at European Consumer and Competition Day: Defending Competition in a Digitised World (Apr. 4, 2019), https://ec.europa.eu/commission/presscorner/detail/en/speech_19_7023 [https://perma.cc/Q455-WWLK].

i. The Misalignment Between Competition Law's Efforts to Decrease Data Concentration and Privacy

The challenges that this approach to promoting competition poses for privacy can be revealed by two forms of regulatory strategy targeted at reducing data barriers to market entry in a way that promotes rival firms, and reduces concentration in data-dependent markets. The first involves requiring market-leading firms with access to critical data to provide access to such data to their rivals. The E.U. Digital Markets Act ("DMA"), effective as of May 2023, which targets large tech companies like Google, Apple, Amazon, and Facebook (Meta), offers an example of this strategy.[51] The DMA includes provisions requiring these "gatekeepers" to make certain data available to competitors—including search data like ranking, query, and click and view data—as a means to overcome "an important barrier to entry and expansion, which undermines the contestability of online search engines."[52]

This requirement reflects earlier enforcement initiatives. For example, in reviewing Apple's 2018 acquisition of Shazam, the European Commission explored requiring Apple to give competitors access to Shazam's data regarding music recommendations and user preferences to ensure that Apple did not use the data to gain an unfair competitive advantage in the digital music streaming market.[53] The European Commission ultimately found an absence of barriers to entry in this market and declined to impose this remedy, concluding that "concerns in that respect were dismissed because Shazam's data is not unique and Apple's competitors would still have the opportunity to access and use similar databases."[54]

Another example of requiring dominant firms to give rivals access to their critical data appears in some of the remedies proposed by the Department of Justice ("DOJ") and state plaintiffs in *United States v. Google LLC* to address Google's unlawful monopoly power in search.[55] The centerpiece of the

51. *See generally* Council Regulation 2022/1925 of 14 September 2022, On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

52. *Id.* at recital 61 and arts. 8–11; U.K. REGULATORS JOINT STATEMENT, *supra* note 28, at 23 ("Some forms of data-related interventions explored in the CMA's market study would seek to promote competition in a market in a targeted way by requiring access to particular types of data for smaller businesses or potential new entrants. The objective would be to ensure that they can compete on a level footing with incumbents that have market power on account of their substantial access to data."); *see also* Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 22–38 (2022) (discussing many examples for how companies used privacy as a pretextual reason not to share data with rivals and other businesses).

53. *See* European Commission Press Release IP/18/3505, *supra* note 31.

54. European Commission Press Release IP/18/5662, Mergers: Commission Clears Apple's Acquisition of Shazam (Sept. 5, 2018), https://ec.europa.eu/commission/presscorner/detail/en/ip_18_5662 [https://perma.cc/2KF6-L2ME].

55. United States v. Google LLC, 747 F. Supp. 3d 1, 187 (D.D.C. 2024) (finding Google liable under Section 2 of the Sherman Act for maintaining monopolies in U.S. general search services and U.S. general search text advertising); *see also* Plaintiffs' Revised Proposed Final

proposal is to ban Google from "providing third parties something of value (including financial payments) in order to make Google the default general search engine or otherwise discourage those third parties from offering competing search products,"[56] like the multibillion-dollar payments Google has made to Apple and other device makers, wireless carriers, and browser developers, which the court found to be exclusionary conduct that violates Section 2.[57] Yet among a broad set of additional proposed remedies,[58] the proposal requires Google to share highly detailed search index data and user-side data—including personal data used to build, create, and operate Google's statistical models, ranking models, or train Google's generative AI models—with certain competitors, and to do so continuously on a periodic basis.[59] In fact, user-side data is defined as "all data that can be obtained from users in the United States, directly through a search engine's interaction with the user's Device, including software running on that Device, by automated means."[60] Before sharing this highly sensitive and voluminous data, under the proposal Google is required to "use ordinary course techniques" to de-identify the data,[61] but it also "must provide sufficient information for each dataset such that it can be reasonably understood" by competitors, including "a description of what the dataset contains, any sampling methodology used to create the dataset, and any anonymization or privacy-enhancing technique that was applied."[62] If adopted, this would create severe privacy problems and harms. De-identification and anonymization techniques are notoriously bad in providing real privacy assurances,[63] and the data that the proposal asks to disseminate is extremely sensitive.[64] Google has urged the court to reject most of the

Judgment at 2, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Mar. 7, 2025), ECF No. 1184-1.

56. *See* Executive Summary of Plaintiffs' Revised Proposed Final Judgment at 7, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Mar. 7, 2025), ECF No. 1184.

57. *See id.* at 2.

58. *Id.* at 7–14.

59. Plaintiffs' Revised Proposed Final Judgment, *supra* note 55, at 14–17.

60. *Id.* at 7. The definition goes on: "User-side Data includes information Google collects when answering commercial, tail, and local queries. User-side Data may also include datasets used to train (at all stages of training including pre-training and filtering, post-training, fine-tuning) Google's ranking and retrieval components, as well as GenAI models used for Google's GenAI Products." *Id.*

61. *Id.* at 17.

62. *Id.*

63. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010); *see also* Caitlin F. Saladrigas, Rachel Marmor, David C. Kully & Ryan Kocse, *Google Search: Data Sharing as a Risk or Remedy?*, HOLLAND & KNIGHT (Apr. 15, 2025), https://www.hklaw.com/en/insights/publications/2025/04/google-search-data-sharing-as-a-risk-or-remedy [https://perma.cc/CNK3-5KYM] ("There is no industry standard that governs this process, and experts, including those assigned to the 'technical committee' that would oversee Google's compliance with the remedy, could easily disagree on implementation.").

64. Saladrigas et al., *supra* note 63 ("As it stands, how would a consumer know if Google were to fail to use 'ordinary course techniques' to remove personally identifiable information?

proposed remedies, including the data-sharing relief.[65] Unsurprisingly, though unfortunate for its privacy effects, in early September 2025, the court ruled on the remedies and, inter alia, "ordered Google to make certain search index and user-interaction data available to rivals and potential rivals."[66]

The second regulatory strategy involves a requirement that consumers be able to "port" their data between platforms, reflecting the regulatory belief in that data portability can promote competition and innovation by removing barriers to users' ability to switch services, and to new entrants' access to markets.[67] Data portability is embedded in leading privacy laws such as the European General Data Protection Regulation ("GDPR")[68] and the California Consumer Privacy Act,[69] as well as in leading competition laws such as the DMA,[70] which all include provisions that promote the ability of users to transfer their personal data from one platform to another.

Setting aside debates over the effectiveness of access to rival firms' data in lowering barriers to entry, or whether user data ported from one platform to another is actually useful to potential competitors—both propositions questioned by scholars of information markets[71]—there are strong reasons to

What mechanisms to police that conduct are available? . . . [A]llowing such data sharing with such limited controls seems almost anachronistic."); Trevor Wagener, *Mandated Tech and Data-Sharing: A Remedy to "Cure" Privacy, Innovation, and U.S. Leadership*, COMPUT. & COMMC'NS INDUS. ASS'N (Mar. 24, 2025), https://ccianet.org/articles/mandated-tech-and-data-sharing-a-remedy-to-cure-privacy-innovation-and-u-s-leadership [https://perma.cc/95HD-BPLT] ("Forcing Google to share its data and its users' data with a broad array of third parties raises serious privacy and national security concerns. The proposed final remedies attempt to handwave away such concerns . . . . For example, Google's search queries and click data include highly sensitive information about individuals' interests, health, location, and communication. . . . Allowing third parties with weaker security standards to access such data vastly increases the potential for misuse.").

65. Plaintiffs' Remedies Post-Trial Brief at 33–34, United States v. Google LLC, No. 20-cv-03010 (D.D.C. May 29, 2025), ECF No. 1369.

66. *See* Press Release, U.S. Dep't of Just., Department of Justice Wins Significant Remedies Against Google (Sept. 2, 2025), https://www.justice.gov/opa/pr/department-justice-wins-significant-remedies-against-google [https://perma.cc/XJS2-Z38L].

67. CHRISTIAN REIMSBACH-KOUNATZE & ANDRAS MOLNAR, OECD, THE IMPACT OF DATA PORTABILITY ON USER EMPOWERMENT, INNOVATION, AND COMPETITION 18 (2024); *see also* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 47–53 (2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 [https://perma.cc/7LY7-AF34] (suggesting that allowing consumers to move data between platforms could benefit competition and consumers).

68. Council Regulation 2016/679 of 27 April 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 20, 2016 O.J. (L 119).

69. California law requires that, on request, businesses must deliver a customer's personal information "in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance." CAL. CIV. CODE § 1798.100[d] (West 2022).

70. *See* Council Regulation 2022/1925, 2022 O.J. (L 265) recitals 36, 59; *id.* at art. 6(9).

71. Gabriel Nicholas & Michael Weinberg, *Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?*, ENGELBERG CTR. ON INNOVATION L. &

think that these regulatory tools in particular (and competition laws' concern with reducing concentration more generally) are a particular mismatch for privacy concerns. This holds true even when this sort of procompetitive requirement from firms is embedded in privacy laws themselves.[72]

At the most basic level, as antitrust scholar Erika Douglas has pointed out, mandated access to data by competitors implicates a fundamental tension with the core data protection principle of individual control over the collection and use of personal information.[73] Regulators have contended that this particular tension between competition and privacy concerns can be resolved by keeping privacy principles in mind when designing competition remedies, such as by mandating only access to data that is "necessary and proportionate," and therefore may not require user consent.[74] Yet mandated access inherently creates direct tension with the core data protection principle of "purpose limitation," the principle that firms should collect personal data only for defined purposes, and should not generally then use that data in ways incompatible with the original purpose.[75] Downstream data sharing is, by default, a deviation from the original purposes of collecting and using the data (unless it was originally declared as a purpose).

The case of data portability rights, while it may not present the same "data autonomy" deficit[76] as mandated access, still carries perhaps the most fundamental set of privacy risks posed by data deconcentration. These risks stem from data portability's inherent tension with the principle of data minimization—the commitment to limiting the collection and processing of information as the core means to lower privacy harms and risks by decreasing the amount of exposure. In the words of U.K. regulators, "data access interventions may be seen as having the potential to create tensions with data protection objectives, for example if they may lead to more widespread processing of personal data by a larger number of controllers."[77] Sharing data

---

POL'Y NYU SCH. L. (Nov. 2019), https://www.nyuengelberg.org/outputs/data-portability-and-platform-competition [https://perma.cc/3WMZ-GXEG].

72. *See* Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIV. L. 250, 258 (2014) (describing data portability as "more at home in the regulation of unfair business practices or electronic commerce, or perhaps competition law—all domains that regulate abuse of power by commercial providers to lock-in consumers").

73. *See* Douglas, *The New Antitrust*, *supra* note 3, at 669.

74. U.K. REGULATORS JOINT STATEMENT, *supra* note 28, at 24.

75. *See, e.g.*, Isabel Hahn, *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, 7 EUR. DATA PROT. L. REV. 31, 32 (2021); Council Regulation 2016/679, art. 5(1)(b), 2016 O.J. (L 119) (explaining that personal data shall be collected for "specified, explicit and legitimate purposes").

76. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 845–55 (2022) (discussing autonomy harms related to privacy); Jiawei Zhang, *The Paradox of Data Portability and Lock-In Effects*, 36 HARV. J.L. & TECH. 657, 664–65 (2023) (discussing data autonomy).

77. U.K. REGULATORS JOINT STATEMENT, *supra* note 28, at 24; *see also* Jan Krämer, *Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations*, 17 J.

with more data controllers, moreover, increases the risk that such data may be illegally accessed or exploited by any one of those firms.

As Professor James Grimmelmann describes, the problem goes well beyond the simple reality that increasing the number of firms aggregating and using an individual's data makes that data both "less secure" and "less private."[78] It enhances what he calls the "horizontal privacy trouble," a phenomenon by which user data—including data about *other* individuals (starting with one's contacts)—can be transferred from one platform to another, stripped "of whatever legal, technical, or social constraints applied to it in social network site *A*," to "social network site *B*," which may or may not have similar restrictions, with "disastrous" privacy consequences.[79]

Importantly, data sharing among rivals or lowering data access barriers generally may increase competition—but in which segment of the economy? The work of economist Jan Krämer and others has demonstrated the ways that lowering data barriers often only increases firms' overall appetite for data collection and use and may thus decrease the incentive to compete *over privacy protections*.[80] Lowering data access barriers may encourage data free riding,[81] and even worse, may lead to a data-value-extraction race to the bottom.

What is good for competition is thus not necessarily good for privacy. Increasing data access among firms in the market harms privacy in foreseeable ways, and to the extent it promotes competition, it does not promote competition *over* privacy protections.

COMPETITION L. & ECON. 263, 276 n.2 (2021) ("[A]s personal data is spread among more data controllers, there is a higher risk that it may be illegally accessed or exploited at one of them.").

78. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1193–95 (2009).

79. *Id.* One could suggest in this situation that the first platform, from which the data is ported, could be required to delete its copy after the port. But we cannot assume that realistically, given what we already know about firms' serious noncompliance with deletion requests. *See* Ella Corren, *Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Rights and Policy Implications*, 109 IOWA L. REV. 2017, 2051 (2024); Alex Hern, *Ashley Madison Database Suggests Paid-Delete Option Left Identifiable Data Intact*, GUARDIAN (Aug. 19, 2015, 4:08 PM), https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-paid-delete-option-left-data-identifying-users-post-claims [https://perma.cc/A5UH-QZ28] ("Date of birth, postcode and other personal data still appear on hacked database of infidelity site – even for accounts that paid for 'full delete' service.").

80. Economist Jan Krämer has also modeled ways in which data portability rights can lead to the collection of more data by reducing both market entrants' and incumbents' incentives to minimize data collection of new customers. *See* Krämer, *supra* note 77, at 273 (market entrants); *see also* Jan Krämer & Nadine Stüdlein, *Data Portability, Data Disclosure and Data-Induced Switching Costs: Some Unintended Consequences of the General Data Protection Regulation*, 181 ECON. LETTERS 99, 99 (2019) (incumbents).

81. *See* Zhang, *supra* note 76, at 678–79.

ii. The Misalignment Between Competition Law's Efforts to Prevent Market Exclusion and Privacy

The reality that concentration in surveillance markets leads to the participation of fewer firms in those markets suggests a reverse misalignment: What is bad for competition may be good for privacy. If data minimization is indeed a cornerstone of privacy, then *more entities* surveilling consumers and citizens is inherently bad for privacy. More competition means more competitors, and more competitors means more data being extracted and used for more purposes and changing more hands in the process.

A real-life example of this misalignment argument arises from competition attacks against market-dominant firms' exclusion of rivals from access to data in the context of "scraping." Scraping is the practice of extracting data from websites or other sources, typically using automated tools or scripts, and has resulted in a number of cases in which competition arguments have been raised to argue that smaller firms should not be barred from scraping information available on dominant platforms. In general, permitting scraping lowers data entry barriers for smaller firms seeking to compete, while prohibiting the practice raises them.

The legal saga of *hiQ Labs, Inc. v. LinkedIn Corp.* is a prominent example. hiQ's business involved collection and analysis of personal data related to people's employment that is posted online.[82] In its lawsuit, hiQ contended that LinkedIn's practice of preventing other firms from scraping data on its platform by placing that data behind code-based access barriers was anticompetitive.[83] LinkedIn's actions clearly had the anticompetitive effect of restricting its rival's access to data the platform has collected. And while the case involved some debate over whether LinkedIn's motives stemmed from an intent to block competitors or, as LinkedIn claimed, a legitimate effort to protect its users' privacy and maintain their trust in the platform,[84] the practice of barring scraping by third parties undoubtedly enhanced user privacy.[85] It limited the number of actors engaged in extracting, sharing, and repurposing users' personal information, and further protected against data exposures and

82. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1103 (N.D. Cal. 2017).

83. *Id.* at 1109–10, 1117–19.

84. *Id.* at 1107 ("LinkedIn's professed privacy concerns are somewhat undermined by the fact that LinkedIn allows other third-parties to access user data without its members' knowledge or consent.").

85. *See* Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 CALIF. L. REV. 1521, 1521 (2025) ("Scraping violates nearly all of the key principles of privacy laws . . . ."); Press Release, ACLU of Ill., In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law (May 9, 2022), https://www.aclu-il.org/en/press-releases/big-win-settlement-ensures-clearview-ai-complies-groundbreaking-illinois-biometric [https://perma.cc/4HZX-ZWGH] (discussing the scraping practices used by Clearview AI in creating its facial recognition software, one of the most notorious and dangerous recent privacy invasions).

the creation of privacy risks and harms to users.[86] As a group of privacy advocates explained, "[p]lacing data behind code-based access barriers is also the only way for LinkedIn to truly protect the privacy of that data."[87]

In the district court's original decision—twice affirmed by the Ninth Circuit[88]—the court recognized the misalignment between privacy and competition. But the court ultimately sided with competition, citing the concern that hiQ "will likely be driven out of business," and refusing to prioritize users' privacy over the lowering of data entry barriers.[89]

Such concerns about the creation of information monopolies and its impact on competition were expressed especially clearly only recently by the District Court for the Northern District of California. The court sided with Bright Data, a smaller market entrant, whose scraping practices X (formerly Twitter) had attempted to prevent. "X Corp.," the court held, "would entrench its own private copyright system that rivals, even conflicts with, the actual copyright system enacted by Congress" and by doing so "would yank into its private domain and hold for sale information open to all, exercising a copyright owner's right to exclude where it has no such right."[90] As Professor Dan Solove recognizes in his important analysis of the privacy-destructive nature of scraping, these cases pit privacy protection against the real competition "concern that if companies can only use data they have, then the big companies will have a tremendous advantage in the development of AI."[91]

iii. The General Misalignment Between Anti-Concentration Efforts and Privacy

The various instances in which what is good for competition is bad for privacy reflect a broader indeterminacy as to whether competition law's efforts to reduce concentration can, or will, align with privacy concerns in any particular case—whether, in Senator Klobuchar's words, "[b]igger is not better" when it comes to privacy as well.[92] To be sure, Big Tech engages in

86. *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1106 ("For its part, LinkedIn argues that it faces significant harm because hiQ's data collection threatens the privacy of LinkedIn users, because even members who opt to make their profiles publicly viewable retain a significant interest in controlling the use and visibility of their data.").

87. Brief of Amici Curiae Electronic Frontier Foundation, DuckDuckGo, and Internet Archive in Support of Plaintiff-Appellee at 15, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783), 2017 WL 5757674.

88. *hiQ Labs, Inc.*, 938 F.3d at 994–95, 998 (holding that, despite the harms to users' privacy interests, LinkedIn's interest in preventing hiQ from scraping those profiles was not "significant enough to outweigh hiQ's interest in continuing its business"), *vacated*, 141 S. Ct. 2752 (2021) (mem.); hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1189–91, 1194 (9th Cir. 2022), *aff'g* 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

89. *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1107 ("In sum, hiQ unquestionably faces irreparable harm in the absence of an injunction, as it will likely be driven out of business.").

90. X Corp. v. Bright Data Ltd., 733 F. Supp. 3d 832, 849–50 (N.D. Cal. 2024).

91. Daniel Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 36 (2025); *see also* Van Loo, *supra* note 52, at 5–6.

92. KLOBUCHAR, *supra* note 13, at 346.

practices that devastate privacy.[93] At the same time, there are credible arguments that data concentration can offer important privacy benefits.

When data collection and usage are concentrated among a few large firms, these entities typically invest more heavily in robust privacy and security measures and standardized practices.[94] As is often the case with compliance more generally, larger firms often have greater resources and increased incentives to implement advanced security technologies and adhere to stringent privacy regulations. That is because these firms might attract more attempts at data breaches as well as more scrutiny from regulators. Google and Meta, despite their controversial practices, often lead the industry in implementing cutting-edge encryption and security infrastructures. This concentration allows for the establishment of comprehensive, uniform data protection standards across a consolidated market.[95] Indeed, research has demonstrated the role of privacy regulation itself in strengthening market-dominant firms, and creating, themselves, barriers to entry.[96] If privacy regulation enhances privacy protections, even if only marginally, it suggests that market concentration could either contribute to or result from such improvements—or perhaps both.

---

93. The enforcement cases we examine in this Article against firms like Facebook and Google are just a few among countless legal proceedings and regulatory actions revealing their anti-privacy business model.

94. *See, e.g.*, *The Big Tech in Cybersecurity Report: How Facebook, Apple, Microsoft, Google, & Amazon Are Tackling Cyber Threats*, CB INSIGHTS (Jan. 11, 2022), https://www.cbinsights.com/research/report/famga-big-tech-cybersecurity [https://perma.cc/5BBR-5MK6] ("[B]ig tech companies . . . are investing heavily in securing their platforms and building cybersecurity products and services.").

95. *See* Sipe, *supra* note 7, at 377 ("Economies of scope are also a factor here; a closed, vertically integrated system naturally presents fewer opportunities for breaches and errors than one in which data must be regularly transferred between and stored among separate entities (perhaps with varying protocols as well). Putting these together, a market with numerous small entities may be less suitable for protecting personal data than a market with fewer large ones.").

96. *See, e.g.*, Alexander Bleier, Avi Goldfarb & Catherine Tucker, *Consumer Privacy and the Future of Data-Based Innovation and Marketing*, 37 INT'L J. RSCH. MKTG. 466, 470 (2020) (providing research that suggests privacy laws like GDPR may advantage incumbent firms, making it more difficult for small or new firms to compete); Michal S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. COMPETITION L. & ECON. 349, 353–55 (2020); Brijesh Pinto, D. Daniel Sokol & Feng Zhu, *The Antitrust and Privacy Interface: Lessons for Regulators from the Data*, 31 GEO. MASON L. REV. 1019, 1026–27 (2024); *see also* Noah Joshua Phillips, Comm'r, FTC, Remarks at the Internet Government Forum USA: Keep It: Maintaining Competition in the Privacy Debate 7–8 (July 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf [https://perma.cc/UM2S-R97N] ("'[I]ronically, big tech companies such as Facebook, Amazon, Apple and Google benefit from a silver lining when it comes to being regulated—what hurts their competitors more only makes them stronger.' That's not ironic—it's economic, exactly how economies of scale work. Resources devoted to compliance can be scaled, and could have been spent on innovation, wages, and so on." (citation omitted)); James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 47–48 (2015) ("Therefore, privacy regulation imposes transaction costs whose effects, our model suggests, will fall disproportionately on smaller firms.").

Without regulation, concentration incentivizes large firms to invest in protecting their data assets to preserve their dominance; as major players, they are more attractive targets for hackers and competitors, and failing to prioritize privacy and security could lead to costly data breaches, financial losses, and diminished user trust. In a regulated environment, moreover, larger firms face heightened scrutiny from regulators, further encouraging investments in compliance. Furthermore, regulation might create barriers to entry for smaller firms that lack the resources to meet stringent compliance requirements, potentially reinforcing the dominance of established players.[97] This multifaceted dynamic illustrates how privacy and market concentration might inversely interact.

Additionally, while corporate surveillance poses serious privacy threats, government surveillance remains a substantial risk as governments increasingly seek to utilize commercial surveillance systems for their own purposes.[98] In this context as well, it appears that concentration does not clearly align along the privacy-interests axis, and could be beneficial for privacy protections. While on the one hand the larger data holdings of certain firms might provide the government greater "one-stop-shop" access, we have seen important instances in which larger firms can use their power to resist law enforcement attempts at privacy incursions when technological "design wars" devolve into a "bilateral court battle between 'government' and the 'private sector.'"[99] This was the case in 2016 when Apple pushed back against the Federal Bureau of Investigation's request that it help break into the encrypted iPhone used by terrorist Syed Rizwan Farook after an attack in San Bernardino, California.[100]

Recently, Apple once again found itself at the center of the tension between these two opposing forces. The fact that the company is big makes it a prime target for government surveillance, but conversely, it also makes it potentially powerful enough to resist and protect user privacy. In February 2025, the British government demanded the creation of a "back door" to access end-to-end encrypted data from Apple users around the world stored in its iCloud service.[101] It required "blanket capability to view fully encrypted material, not merely assistance in cracking a specific account" though such a

97. *See* sources cited *supra* note 96.

98. *See* Yan Fang, *Internet Technology Companies as Evidence Intermediaries*, 110 VA. L. REV. 1227, 1229 (2024) (describing how government actors use the law to gather information from internet technology companies as evidence).

99. Deirdre K. Mulligan & Kenneth A. Bamberger, *Apple v. FBI: Just One Battle in the 'Design Wars,'* LAW.COM (Mar. 18, 2016, 7:26 PM), https://web.archive.org/web/20210513095815/http:/www.law.com/sites/lawcomcontrib/2016/03/18/apple-v-fbi-just-one-battle-in-the-design-wars (on file with the *Iowa Law Review*).

100. *Id.*

101. Joseph Menn, *U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts*, WASH. POST (Feb. 7, 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk (on file with the *Iowa Law Review*).

requirement "has no known precedent in major democracies."[102] The technology at issue is cloud storage that only the user, and not Apple, can unlock, called Advanced Data Protection ("ADP").[103] ADP enhances hacking protection and, importantly, blocks a common law-enforcement tactic: serving secret search warrants on Apple to access iCloud photos, messages, and other data which, absent the ADP, can be served without the user knowing.[104] As a result, later that month Apple removed its highest level of privacy protection, ADP, from users in the United Kingdom.[105] Apple was targeted due to its size and, for now, has lost the privacy battle. However, as a powerful and resourceful tech giant, it is well positioned to appeal the case—and has done so.[106]

As Professor Matthew Sipe has written, "[i]t is difficult to imagine, for example, a firm with less clout than Apple successfully resisting federal investigators' demands to weaken product security and install abusable backdoors."[107] Thus, in his words, privacy "faces a problem of smallness: Personal data privacy is likely not better served by a multiplicity of small, independent firms."[108]

To summarize the first category of arguments, where data is considered a business asset: Although there are uncommon instances—particularly in the context of regulatory merger reviews—where restricting the combination of datasets simultaneously curbs market power and protects privacy, these alignments are exceptional and fragile. In practice, competition remedies that increase access to data are more conventional and they tend to erode privacy protections, while greater concentration in surveillance markets, though anti-competitive, may actually reduce privacy harms by limiting the number of actors engaged in data extraction. Overall, what advances competition does not reliably advance privacy, and the two regulatory aims often pull in opposite directions.

B. Competition Arguments About Privacy-as-Quality and Surveillance-as-Price

While the previous Section explored concerns arising from data as a business asset, reflecting a lens by which privacy law operates exogenously to competition, this Section addresses competition arguments that treat privacy as an endogenous component of the quality or price of the service being

102. *Id.*

103. Zoe Kleinman, *Apple Pulls Data Protection Tool After UK Government Security Row*, BBC (Feb. 22, 2025), https://www.bbc.com/news/articles/cgj54eq4vejo [https://perma.cc/X9DA-ABAB].

104. *Id.*

105. Kleinman, *supra* note 103; *Apple Can No Longer Offer Advanced Data Protection in the United Kingdom to New Users*, APPLE (Sept. 23, 2025), https://support.apple.com/en-gb/122234 [https://perma.cc/B8CE-KJZ4].

106. Tim Bradshaw & Lucy Fisher, *Apple Launches Legal Challenge to UK 'Back Door' Order*, FIN. TIMES (Mar. 4, 2025), https://www.ft.com/content/3d8fe709-f17a-44a6-97ae-f1bbe6dodccd (on file with the *Iowa Law Review*).

107. Sipe, *supra* note 7, at 375–76.

108. *Id.* at 389.

offered.[109] Competition law has traditionally focused on increased prices and reduced output as the typical negative effects of market power accumulation and, more recently, has also looked at negative impacts on quality and consumer choice.[110] Privacy considerations and the role personal data may play in driving those harmful effects have usually garnered little attention.[111]

This, however, has been changing significantly[112] with the growing recognition among regulators and scholars that personal information is the real engine (or the new "oil," or "currency") of the multibillion-dollar targeted advertising industry.[113] This industry has become the backbone of the internet and digital markets more broadly. The leading business model in digital markets is the extraction and monetization of personal information, which then fund a vast array of "free" content, products, and services that firms in these markets generate and provide.[114] That said, paid-for content, products, and services are no exception—they too collect and monetize personal information.[115] The targeted-advertising industry has become so successful that its logic has infiltrated even firms relying on direct purchase or subscription models.[116] This economic reality suggests that firms dominating the supply side of personal information and its sophisticated analytics could create significant barriers to competition.[117] The growing trend of data-rich mergers and acquisitions,

109. *See* Samson Y. Esayas, *Privacy-as-a-Quality Parameter of Competition*, *in* COMPETITION LAW FOR THE DIGITAL ECONOMY 126, 126–27 (Björn Lundqvist & Michal S. Gal eds., 2019).

110. *Id.* at 127.

111. *Id.* at 127–28.

112. *Id.*

113. *See, e.g.*, Emilio Calvano & Michele Polo, *Market Power, Competition and Innovation in Digital Markets: A Survey*, 54 INFO. ECON. & POL'Y 1, 10–11 (2021); JOHN DEIGHTON & LEORA KORNFELD, INTERACTIVE ADVERT. BUREAU, THE SOCIOECONOMIC IMPACT OF INTERNET TRACKING 3–4 (2020), https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf [https://perma.cc/ER6Y-SSWR].

114. *See* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 42 (2019); Esayas, *supra* note 109, at 127–30; EUR. COMM'N, CASE NO COMP/M.5727 –MICROSOFT/YAHOO! SEARCH BUSINESS ¶ 33 (Feb. 18, 2010) [hereinafter MICROSOFT/YAHOO! SEARCH BUSINESS EC MERGER REVIEW], https://ec.europa.eu/competition/mergers/cases/decisions/M5727_20100218_20310_261202_EN.pdf [https://perma.cc/X7T6-FPHQ] (describing that "internet search services are today generally provided free of charge to users," and that "[s]earch engines are financed by advertising revenue generated by search advertisements").

115. Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327, 330–36 (2020) (discussing the model of paid services).

116. *See, e.g.*, GIRARD KELLY, JEFF GRAHAM, JILL BRONFMAN & STEVE GARTON, PRIVACY OF STREAMING APPS AND DEVICES: WATCHING TV THAT WATCHES US 2 (2021), https://www.commonsensemedia.org/sites/default/files/research/report/privacy_of_streaming_apps_and_devices-final.pdf [https://perma.cc/B54C-6FGJ] (demonstrating that even subscription-based services that one pays for, like YouTube TV, Amazon Prime, and Netflix, collect and process personal information for monetization).

117. *See* Srinivasan, *supra* note 114, at 43 ("Facebook's power [in the digital advertising market] is so absolute that the duopoly of Facebook and Google accounts for 90-99% of year-over-year

which consolidate immense repositories of personal data alongside considerable market power in the hands of a few firms, underscores the potential interplay between privacy and competition, and increasingly challenges the traditional perspective that privacy is irrelevant to competition law.[118]

This Section explores scenarios in which competition concerns about privacy as a component of quality align, and misalign, with privacy protection. The first scenario involves the situation in which, as one of this Article's Authors previously described, market power can "eliminate competitive pressure on platforms to improve quality along the privacy–protective dimension—and even offer them substantial leeway to adopt significantly less privacy–protective practices without market pushback."[119] In these situations—where users are "locked in" to a particular firm or platform despite poor, or even worsening, privacy practices—competition and privacy arguments align. The second scenario arises when dominant firms engage in behaviors that promote privacy by excluding or disadvantaging rivals—a so-called "gatekeeper" situation—but, by doing so, they harm competition. Here, privacy and competition not only misalign, but conflict.

1. Aligned Concerns About Market-Dominant Firms: Privacy Lock-In

Understanding the privacy lock-in argument requires adoption of a particular conception of privacy as a commercial, material, and marketable good[120] in two senses. First, privacy contributes to the overall quality of a product or service.[121] A product designed with stronger privacy protections is perceived as higher quality, whereas a product with weaker privacy protections—or none at all—is viewed as lower quality. In simple terms: Strong privacy is a feature, while weak privacy is a bug.[122]

---

growth in the U.S. digital advertising market."); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 359–65 (2022).

118. Esayas, *supra* note 109, at 128–29 (describing how that recent trebling of data mergers "ushers in a new challenge on whether, and if so to what extent, privacy is a concern in competition law assessments when companies in data-rich industries seek a merger or acquisition").

119. Bamberger & Lobel, *supra* note 7, at 1089–90.

120. *See generally* Jan Whittington & Chris J. Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327 (2012) (exploring how personal data is exchanged and monetized).

121. *See, e.g.*, Esayas, *supra* note 109, at 130; Francisco Costa-Cabral & Orla Lynskey, *Family Ties: The Intersection Between Data Protection and Competition in EU Law*, 54 COMMON MKT. L. REV. 11, 29–30 (2017).

122. *See, e.g.*, Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, COMPETITION POL'Y INT'L ANTITRUST CHRON. 5–6 (May 29, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2617685 [https://perma.cc/986N-LKB7] (discussing trade-offs between privacy and other product quality dimensions); Douglas, *The New Antitrust*, *supra* note 3, at 657–58 ("This non-complementarity . . . raises a variation on the familiar question of how to evaluate tradeoffs between different dimensions of product quality. Product design changes may cause privacy to decrease, but at the same time, improve other elements of product quality. . . . How does antitrust analysis evaluate the effects on consumer welfare when there are multiple different dimension[s] of quality?" (footnote omitted)).

Second, information privacy can be factored into the actual price consumers pay for products and services.[123] A product that extracts more personal information from a user effectively "costs" the user more than one that extracts less.[124] This is because personal information holds monetary value for firms in the information economy—whether it is directly sold to data merchants and brokers or monetized through the targeted-advertising ecosystem[125]—as well as because personal information carries economic, emotional, and dignitary value for the users from whom it is extracted.[126] Surveillance may also indirectly affect "regular" prices consumers are paying for goods and services by feeding algorithms used for price discrimination and price gouging.[127]

To put these two forms of privacy-as-a-good together: A lack of privacy is equivalent to *lower quality* and *higher prices* for products and services in the market. If privacy can be conceptualized and quantified in market terms—as a determinant of quality and price—then competition can, at least in theory, play a central role in shaping its availability and value. In a highly competitive market, we should expect to see greater output in the form of stronger privacy protections and lower price extraction in the form of reduced surveillance.

---

123. *See* Esayas, *supra* note 109, at 130; Peter P. Swire, Senior Fellow, Ctr. for Am. Progress, Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall 1 (2007), https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf [https://perma.cc/84NH-JG8F].

124. *See* Gregory Crawford, Johnny Ryan & Cristina Caffarra, *The Antitrust Orthodoxy Is Blind to Real Data Harms*, CTR. FOR ECON. POL'Y RSCH. (Apr. 22, 2021), https://cepr.org/voxeu/blogs-and-reviews/antitrust-orthodoxy-blind-real-data-harms [https://perma.cc/33QJ-W3H9] (characterizing privacy features, and the loss of privacy or lack of data protection that comes with their relaxation, as "price"); Viktoria H.S.E. Robertson, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data*, 57 COMMON MKT. L. REV. 161, 173–78 (2020) (arguing that E.U. competition law could prohibit excessive data collection by analogizing it to excessive prices).

125. *See* Derek E. Bambauer, *Target(ed) Advertising*, 58 U.C. DAVIS L. REV. 1429, 1467, 1468 n.217, 1471–72 (2025); Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, Online Tracking and Publishers' Revenues: An Empirical Analysis 2–5 (May 2019) (unpublished manuscript), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf [https://perma.cc/NJ9H-ZN28]. *See generally* Eduardo Abraham Schnadower Mustri, Alessandro Acquisti & Idris Adjerid, Behavioral Advertising and Consumer Welfare (Sept. 2024) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398428 [https://perma.cc/AKZ5-4T62] (evaluating consumer welfare implications of behavioral advertising made possible by personal data collection).

126. *E.g.*, Citron & Solove, *supra* note 76, at 830–61.

127. *See, e.g.*, Irina Ivanova, *Delta Moves Toward Eliminating Set Prices in Favor of AI that Determines How Much You Personally Will Pay for a Ticket*, FORTUNE (July 23, 2025, 6:50 PM), https://fortune.com/2025/07/16/delta-moves-toward-eliminating-set-prices-in-favor-of-ai-that-determines-how-much-you-personally-will-pay-for-a-ticket [https://perma.cc/3EJ5-GRAN] ("Delta has a long-term strategy to boost its profitability by moving away from set fares and toward individualized pricing using AI. The pilot program, which uses AI for 3% of fares, has so far been 'amazingly favorable,' the airline said. Privacy advocates fear this will lead to price-gouging, with one consumer advocate comparing the tactic to 'hacking our brains.'. . . Sen. Ruben Gallego (D-Ariz.) called Delta's practice 'predatory pricing' . . . ."); *see also infra* note 201 and accompanying text (discussing how privacy protections may prevent price discrimination).

These are the core benefits that market competition is intended to deliver to consumers.[128]

Conversely, the absence of competition over privacy-as-a-good results in low quality and high prices. This scenario is what we term a privacy lock-in, where consumers are trapped in poor privacy conditions, either at the level of a single firm or across the entire market. Firm-level privacy lock-in occurs when consumers rely on a product or service that is difficult to replace, often due to factors like network effects. Market-level privacy lock-in arises when most or all firms within an industry offer poor privacy conditions, effectively eliminating competition on the privacy parameter.[129] In both cases, privacy lock-in deprives consumers of meaningful choice, driven by a lack of market competition over privacy-as-a-good.[130]

The privacy-as-a-good approach—encompassing the mirror conceptions of privacy-as-quality and surveillance-as-price—is becoming increasingly prevalent in competition enforcement. In 2010, the European Commission reviewed the proposed merger of Microsoft and Yahoo, which involved Microsoft taking over Yahoo's search business.[131] The European Commission found that in the case of "free" products and services, such as online search, the quality of the "free" good becomes a primary source of competition.[132]

Later merger review decisions embraced this notion and highlighted the fact that the quality parameter might specifically consider privacy. In the case of the 2014 Facebook–WhatsApp merger, the European Commission found that consumer communication apps like Facebook Messenger and WhatsApp primarily compete on two factors: app functionalities and network size.[133] Among functionalities, the European Commission emphasized the growing

128. Esayas, *supra* note 109, at 127–28.

129. *Id.* (discussing the effect of market power on increasing prices and reducing quality). Margaret Radin discusses a parallel phenomenon by which firms adopt identical boilerplate practices, so that only one level of quality "occup[ies] the territory in which a consumer is participating." MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 41–42 (2013). She argues that such a "[c]opycat boilerplate" phenomena "should be evaluated as a possible form of tacit collusion," because it similarly restricts choice in a market. *Id.* at 41. "Industry-wide standardization of a boilerplate scheme prevents consumers from choosing terms they would prefer. They have no exit from onerous terms. Moreover, industry-wide standardization may result in a market in which firms offer the least favorable terms they can get away with." *Id.* at 42.

130. *See* Esayas, *supra* note 109, at 129; STUCKE & GRUNES, *supra* note 3, at 61 ("The reason why market forces have not yielded the privacy protections that we desire is the *absence* of meaningful competition."); *see also* Swire, *supra* note 123, at 5 ("My point . . . is that this sort of [loss of privacy] is a logical component of antitrust analysis."); Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 797 (2010) (arguing the FTC should "recognize and explore the nexus between competition and privacy").

131. MICROSOFT/YAHOO! SEARCH BUSINESS EC MERGER REVIEW, *supra* note 114, ¶¶ 13, 26.

132. *Id.* ¶ 101.

133. FACEBOOK/WHATSAPP EC MERGER REVIEW, *supra* note 39, ¶ 86.

importance of "privacy and security," citing the rise of apps specifically targeting these concerns,[134] and WhatsApp's and Facebook's decision to avoid introducing ads on WhatsApp post-transaction—which would have entailed behavioral surveillance and erosion of privacy.[135] It also noted that higher-quality functionalities are central to the value these apps offer, and are thus critical to attracting the largest user base.[136] These findings acknowledge privacy as a marketable good and highlight the risk of privacy lock-in if competition is restricted. Two years later, when considering the 2016 Microsoft–LinkedIn merger, the European Commission further expanded its view, recognizing privacy as a key competitive factor warranting market analysis,[137] and acknowledging the risk that anticompetitive effects could marginalize competitors offering stronger privacy protections or hinder the entry of such competitors.[138]

Fast forward a few years and the American regulator, the FTC, not only recognized the privacy-as-quality approach, but included it as part of its broader argument for breaking up Facebook due to its anticompetitive conduct.[139] As technology-markets scholar Dina Srinivasan's work has described, Facebook had created, step-by-step, surreptitiously and purposefully, a degraded privacy lock-in environment by marginalizing competition and silencing users.[140] In the absence of competition, the market reality created by Facebook ultimately diminished consumer welfare, and enabled "a monopolist to offer inferior quality products."[141] In the FTC's complaint against Facebook, filed in the U.S. District Court for the District of Columbia, the FTC argued among other things that Facebook's acquisitions of WhatsApp and Instagram enabled the platform to dominate the personal social media services market, resulting in an intentional decline in consumer privacy unconstrained by competition.[142] The FTC further argued that "Facebook's ability to harm users by decreasing product quality [in the form of privacy protections], without losing significant

134. *Id.* ¶ 87.

135. *See id.* ¶¶ 168–70.

136. *Id.* ¶ 87.

137. EUR. COMM'N, CASE NO COMP/M.8124 - MICROSOFT/LINKEDIN ¶¶ 348–50 (Dec. 6, 2016) [hereinafter MICROSOFT/LINKEDIN EC MERGER REVIEW], https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf [https://perma.cc/74M9-ERCY].

138. *Id.*; *see also* SAMSON Y. ESAYAS, DATA PRIVACY AND COMPETITION LAW IN THE AGE OF BIG DATA: UNPACKING THE INTERFACE THROUGH COMPLEXITY SCIENCE 197 (2024).

139. Press Release, FTC, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (Aug. 19, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed [https://perma.cc/J9KV-WSVM].

140. *See generally* Srinivasan, *supra* note 114.

141. *Id.* at 43.

142. First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 105, 127, FTC v. Facebook, Inc., 560 F. Supp. 3d 1 (D.D.C. 2021) (No. 20-cv-03590), 2020 WL 14046541 [hereinafter FTC 2021 Facebook Complaint].

user engagement, indicates that Facebook has market power."[143] Thus, the FTC not only recognized privacy degradation as a consequence of Facebook's monopolistic behavior, but also as the evidence of the company's dominant position, warranting regulatory intervention.

The FTC complaint highlights that WhatsApp's success was driven by its strong privacy features, which were undermined after its acquisition by Facebook.[144] Thus, according to the complaint, the merger eliminated a privacy-focused alternative, replacing it with increased data collection and broader data use in line with Facebook's surveillance business model.[145] Therefore, beyond demonstrating Facebook's market power, this move to constrain market options for privacy also effectuated privacy lock-in.[146]

2. Misaligned Concerns Regarding Practices that Might Improve Privacy, but Harm Competition: The Gatekeeper Scenario

The lock-in approach offers a strong example of the ways that conceiving of privacy as a classic economic good can bring competition and privacy concerns into alignment. Conceptualized as a quality parameter with price implications—and subject to competition or a lack thereof—privacy protection *can* (at least conceptually) be cleanly integrated into conventional competition frameworks. Thus, to the extent firms compete on privacy, removing barriers to competition could promote both values.

However, recognizing privacy as a component of product and service quality over which firms have control has also cut the other way. In these contradictory contexts, regulators express concern over the ways that market-dominant firms could use privacy-protective measures as an anticompetitive means to exclude rivals.[147] By this analysis, competition and privacy values are inversely correlated.

This tension reflects the structure of digital markets and the surveillance economy. Dominant tech firms like Apple, Google, and Meta are often viewed as "gatekeepers" due to their control over entire platforms and networks connecting consumers and businesses.[148] This position grants them significant power, enabling potential anticompetitive behavior that can influence entire markets.[149] Simultaneously, however, these firms also possess, at least

143. *Id.* ¶ 207.

144. *Id.* ¶¶ 113, 127.

145. *Id.*

146. Esayas, *supra* note 109, at 203; *see also* New York v. Facebook, Inc., 549 F. Supp. 3d 6, 23 (D.D.C. 2021), *aff'd sub nom.* New York v. Meta Platforms, Inc., 66 F.4th 288 (D.C. Cir. 2023).

147. *See, e.g.*, MICROSOFT/YAHOO! SEARCH BUSINESS EC MERGER REVIEW, *supra* note 114, ¶ 33.

148. *Gatekeepers*, EUR. COMM'N, https://digital-markets-act.ec.europa.eu/gatekeepers_en [https://perma.cc/5X5S-PZQN] ("On 6 September 2023 the European Commission designated for the first time six gatekeepers - Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft - under the Digital Markets Act . . . .").

149. Like in the Facebook case. *See supra* notes 133–46 and accompanying text; *see also* Peter Ormerod, *Privacy Law's Incumbency Problem*, 58 U.C. DAVIS L. REV. 179, 202 (2024).

theoretically, the ability to establish higher quality standards, including in privacy, thereby driving improved practices across the industry. When dominant firms leverage their market power to enforce stricter privacy standards on businesses operating within their platforms, market concentration that underpins their dominance becomes a driving force for the implementation of better privacy protections. In this scenario, then, the misalignment between competition and privacy arises even though privacy is considered a marketable good and not merely a force that is exogenous to the market.

From a pure competition perspective, a gatekeeper firm is suspicious and prone to anticompetitive behavior that could facilitate market failure. For example, the DMA, Europe's recently enacted competition framework, defines gatekeeper firms as those that provide "core platform services" such as search engines, social networks, video-sharing platforms, operating systems, and web browsers.[150] The DMA adopts a critical perspective on so-called gatekeeper firms, highlighting qualities that can undermine competition. These include extreme economies of scale,[151] strong network effects,[152] lock-in mechanisms, limited multi-homing,[153] vertical integration, and data-driven advantages.[154] Such characteristics can confer gatekeeping firms with the ability to diminish competition and fairness through their interactions with businesses and end users, ultimately restricting consumer choice.[155] The DMA addresses concerns about the ability of gatekeepers to restrict critical gateways between businesses and consumers by introducing measures to curb their power, prevent unfair

150. Council Regulation 2022/1925, art. 2(1–2), 2022 O.J. (L 265).

151. *Id.* at recital 2 (describing that these "often result from nearly zero marginal costs to add business users or end users").

152. *Id.* (describing that this relates to "an ability to connect many business users with many end users through the multisidedness of these services, a significant degree of dependence of both business users and end users").

153. For a definition of multi-homing in the context of the digital economy, see, for example, EUR. COMM'N, MULTI-HOMING: OBSTACLES, OPPORTUNITIES, FACILITATING FACTORS 8 (2021) ("Multi-homing refers to a situation in which users tend to use several competing platform services in parallel. This applies to all sides of the market: businesses using different platforms to sell their goods and services; customers (buyers, end users) switching between different platforms to buy the goods and services that they need. Multi-homing may help to counter the network effects and subsequent economic power that large platforms benefit from. If business users as well as their customers could easily change platforms or use several platforms in parallel without significant costs and inconveniencies, this would make markets more competitive and decrease the economic power of large platforms. It could lower barriers to entry for emerging new platforms and foster innovation.").

154. *Id.*

155. Council Regulation 2022/1925, 65 O.J. (L 265) recitals 2–3 (discussing undertakings that "exercise control over whole platform ecosystems in the digital economy and are structurally extremely difficult to challenge or contest by existing or new market operators, irrespective of how innovative and efficient those market operators may be").

practices, and promote openness in important digital services.[156] Such mechanisms include formally designating gatekeeper firms in specific markets once they meet defined thresholds,[157] and imposing strict conduct requirements with a clear list of regulator-defined obligations and prohibitions.[158] As the most advanced regulatory framework for tackling anticompetitive behavior in digital markets, the DMA stands out not only for its ability to address past issues but also for its forward-looking rules designed to proactively prevent future market failures.

The DMA's distrustful posture toward gatekeeper firms is clear and aligns with traditional competition concerns. But, at least in some cases, gatekeepers' noncompetitive behavior can be pro-privacy and pro-consumer.

The scenario in which a gatekeeper firm might use its market power to promote privacy involves the adoption of practices resulting in the exclusion, or differential treatment, of businesses on the platform based on their data practices. Apple, for example, points to such privacy-protective justifications regarding its App Tracking Transparency ("ATT") feature.[159] ATT creates new consent and notification requirements that change the way app developers can collect and use consumer data for mobile advertising on iOS, such as by providing an "Ask App Not to Track" prompt. This has, in the words of one commentator, "upended the mobile ad industry, which is built on data, by abruptly cutting off one of its streams."[160] It certainly made Meta, another gatekeeper, nervous, prompting the company to acknowledge that this change in privacy settings would have a significant financial impact "on the order of $10 billion . . . for our business."[161]

---

156. European Commission Press Release IP/23/4328, Digital Markets Act: Commission Designates Six Gatekeepers (Sept. 6, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 [https://perma.cc/F38D-Y9Q2].

157. *Id.*

158. *Id.*

159. Sara Morrison, *The Winners and Losers of Apple's Anti-tracking Feature*, VOX (Apr. 29, 2022, 12:00 PM), https://www.vox.com/recode/23045136/apple-app-tracking-transparency-privacy-ads (on file with the *Iowa Law Review*).

160. *Id.* (quoting Meta CFO Dave Wehner).

161. Kif Leswing, *Facebook Says Apple iOS Privacy Change Will Result in $10 Billion Revenue Hit This Year*, CNBC (Feb. 2, 2022, 7:54 PM), https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html [https://perma.cc/9H2V-C4LY]; *see also* Van Loo, *supra* note 52, at 103 n.7 (observing that Facebook commissioned an analysis of Apple's privacy emphasis and alleged anticompetitive conduct). Yet, Meta did not let this derail its tracking empire—reports soon emerged that Apple's new feature could be, and was being, circumvented. *See* Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns & Nigel Shadbolt, *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels*, PROC. 2022 ACM CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY 508, 508 (2022); Dan Goodin, *Your iOS App May Still Be Covertly Tracking You, Despite What Apple Says*, ARSTECHNICA (Apr. 19, 4:10 PM), https://arstechnica.com/information-technology/2022/04/a-year-after-apple-enforces-app-tracking-policy-covert-ios-tracking-remains [https://perma.cc/UU9S-XH9E]. And it wasn't long before Meta faced a lawsuit for allegedly bypassing Apple's privacy safeguards in secret. *See* Jovi Umawing, *Facebook Users Sue Meta for Allegedly Building "Secret Workaround" to Apple Privacy*

In 2021, the French Competition Authority ("FCA") first reviewed Apple's ATT feature after advertisers complained that the pro-privacy feature would be "an abuse of a dominant position on the part of Apple, leading to imposing unfair trading conditions to application developers."[162] The FCA rejected the request for interim measures but said it will continue to investigate the case.[163] In March 2025, however, the FCA changed its mind and decided to impose a €150 million fine on Apple for abusing its dominant position through the implementation of "artificially" complicated requirements for obtaining user consent to tracking.[164] Although according to Apple the ATT feature "was designed as an interface using simple, standardised wording to facilitate user information and choice as regards third-party tracking,"[165] the FCA noted that consent obtained through the ATT is not considered valid under the GDPR, "meaning that app publishers must display at least a second consent window . . . to authorise third-party tracking on apps downloaded to an iPhone or iPad."[166] On the basis of that, the FCA found that the ATT feature was disproportionate to achieving Apple's privacy goals, as publishers must deploy separate consent pop-ups, creating complexity and undermining choice "neutrality" by requiring consent to be confirmed twice while refusal only once.[167] This "asymmetry," the FCA opined, disproportionately harms publishers reliant on advertising and particularly disadvantages smaller publishers while Apple retains access to large quantities of proprietary personal data unaffected by the ATT.[168]

Apple's ATT tool undoubtedly improved privacy protection—thereby creating strong incentives for a legal attack. Yet from a competition perspective, it was readily found to constitute an abuse of a dominant market position and was therefore unlawful. Competition debates regarding Apple's app privacy practices more generally arose in another recent dispute between the company and a competitor called Tile. Tile produces tracking devices for items such as phones, backpacks, and keys. Representatives of the company

---

Safeguards, MALWAREBYTES LABS (Sept. 27, 2022), https://www.malwarebytes.com/blog/news/2022/09/facebook-users-sue-meta-for-attempting-to-bypass-apple-privacy-safeguards [https://perma.cc/GA37-GJ8Z].

162. *Targeted Advertising: No Urgent Interim Measures Against Apple but the Autorité Continues to Investigate into the Merits of the Case*, AUTORITÉ DE LA CONCURRENCE (Mar. 17, 2021), https://www.autoritedelaconcurrence.fr/en/article/targeted-advertising-no-urgent-interim-measures-against-apple-autorite-continues [https://perma.cc/793H-F3T7].

163. *Id.*

164. AUTORITÉ DE LA CONCURRENCE, DECISION 25-D-02 OF 31 MARCH 2025 REGARDING PRACTICES IMPLEMENTED IN THE SECTOR FOR MOBILE APPLICATION ADVERTISING ON IOS DEVICES 4, 97 (Mar. 31, 2025), https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2025-07/25d02_public_version.pdf [https://perma.cc/57Z9-QLE4].

165. *Id.* at 3.

166. *Id.*

167. *Id.* at 4.

168. *Id.*

testified before Congress multiple times in 2020 and 2021, complaining that Apple's conduct excluded them from the market, and also arguing that Apple significantly limited Tile's ability to compete with Apple over location-based tracking services because Apple had announced its own competing service with its AirTag device.[169] Among other claims, Tile argued that Apple inserted friction into the relationship between Tile and its consumers by making it difficult for consumers to allow Tile access to their location data by, for example, requiring users first to enable the "Always Allow" setting.[170] This friction did not exist when using Apple's own location-based tracking service.[171] To level the playing field, Tile advocated for loosening default privacy settings, relying on most users to not change them.[172]

In response, Apple claimed that its actions were directed at improving user privacy—making sure users properly authorize and control location tracking, and that they understand "how their data is used" while allowing them to "limit the amount of data companies can collect or sell."[173] Apple also stingingly noted that "[s]tronger privacy protections may not be in everyone's business interest, but they are in the interest of every person with a

169. *See Online Platforms and Market Power, Part 5: Competitors in the Digital Economy: Hearing Before the Subcomm. on Antitrust, Com. & Admin. L. of the H. Comm. on the Judiciary*, 116th Cong. 39–40 (2020) (statement of Kirsten Daru, Chief Privacy Officer and General Counsel, Tile, Inc.), https://docs.house.gov/meetings/JU/JU05/20200117/110386/HHRG-116-JU05-Wstate-DaruK-20200117-U1.pdf [https://perma.cc/N89F-SVW5].

170. *Id.* at 43.

171. *Id.* at 3 ("It made it difficult for consumers to enable their Tile devices. They did this by burying required permissions (called 'Always Allow') deep within the iOS settings; Once permissions are enabled, Apple also began sending frequent prompts encouraging our customers to turn them off, causing customer frustration and implying that Tile shouldn't be trusted." (internal citations omitted)); *see also id.* (arguing that changes in Apple's permissions protocol "increased the 'friction' a user faces when initializing and using third-party apps, while simultaneously decreasing the relative friction for (and transparency of) Apple's own location tracking services"); *Antitrust Applied: Examining Competition in App Stores: Hearing Before the Subcomm. on Competition Pol'y, Antitrust, and Consumer Rts. of the S. Comm. on the Judiciary*, 117th Cong. 6–8 (2021) (statement of Kirsten Daru, Chief Privacy Officer and General Counsel, Tile, Inc.), https://www.judiciary.senate.gov/imo/media/doc/04.21.21%20Kirsten%20Daru%20Senate%20Judiciary%20Testimony%20Final.pdf [https://perma.cc/2GSQ-K9WU] (complaining, among other issues, about Apple's user permission system creating obstacles to Tile's access to user location data).

172. *Antitrust Applied: Examining Competition in App Stores*, *supra* note 171, at 13; *see also* Sipe, *supra* note 7, at 396 (discussing the Tile case).

173. Letter from Kyle Andeer, Vice President, Corp. L. & Chief Compliance Officer, Apple Inc., to Hon. Jerrold Nadler, Chairman, H. Comm. on the Judiciary, Hon. Doug Collins, Ranking Member, H. Comm. on the Judiciary, Hon. David N. Cicilline, Chairman, Subcomm. on Antitrust, Com. & Admin. L. of the H. Comm. on the Judiciary, and Hon. F. James Sensenbrenner, Ranking Member, Subcomm. on Antitrust, Com. & Admin. L. of the H. Comm. on the Judiciary 3 (Feb. 17, 2020), https://docs.house.gov/meetings/JU/JU05/20200117/110386/HHRG-116-JU05-20200117-SD004.pdf [https://perma.cc/5A6B-NVJN] ("We believe our users have a right to know when an app uses their location data before they decide to share it indefinitely.").

smartphone."[174] Further, Apple pointed to privacy-enhancing distinctions between the way its own apps handle location data compared to others, including storing data on the device itself and not externally, thereby minimizing user privacy risks in contrast to Tile and others.[175]

Apple has consistently highlighted its commitment to privacy in its branding, and is often recognized for its privacy-focused products.[176] At the same time, its general data extraction practices have also been severely criticized for their capaciousness,[177] and Tile argued before Congress that Apple's privacy justifications in this case were merely pretextual.[178] This echoed the claim that hiQ had made about LinkedIn's arguments in its challenge discussed previously,[179] and that numerous antitrust commentators and courts have leveled against privacy justifications for anticompetitive conduct elsewhere.[180]

---

174. *Id.*

175. *See id.* (explaining that local storage "provides enormous benefit to our users' security and privacy"). Subsequently, Apple addressed some of the competition concerns raised by Tile and others by introducing interoperability into its FindMy app, allowing third-party products and tracker devices to be located in a manner similar to Apple's own products. *See* STAFF OF H. COMM. ON THE JUDICIARY, SUBCOMM. ON ANTITRUST, COM. & ADMIN. L. OF THE COMM. ON THE JUDICIARY, 117TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 55, 358 n.2274 (2020), https://democrats-judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf [https://perma.cc/S7UH-6VSD] (citing Ben Lovejoy, *Comment: This Week's Keynote Quietly Tackled Five of Apple's Antitrust Issues*, 9TO5MAC (June 24, 2020, 7:23 AM), https://9to5mac.com/2020/06/24/apples-antitrust-issues-2 [https://perma.cc/EP6T-CFE6]); Andrew O'Hara, *Apple Starts Allowing Third-Parties to Join the Find My App Ahead of 'AirTags' Launch*, APPLEINSIDER (Jan. 11, 2021, 1:03 PM), https://appleinsider.com/articles/21/01/11/apple-starts-allowing-third-parties-to-join-the-find-my-app-ahead-of-airtags-launch [https://perma.cc/3T7E-YMDX]. But Tile remained unhappy about this solution because it restricted it from using its own app as part of its tracking service. SUBCOMM. ON ANTITRUST, *supra*, at 55, 358 ("Apple's solution would continue to put Tile and other apps and hardware developers offering finder services at a competitive disadvantage.").

176. Letter from Kyle Andeer, Vice President & Chief Compliance Officer, Apple Inc., to Hon. Amy Klobuchar, Chair, S. Judiciary Comm. Subcomm. on Competition Pol'y, Antitrust & Consumer Rts., and Hon. Mike Lee, Ranking Member, S. Judiciary Comm. Subcomm. on Competition Pol'y, Antitrust & Consumer Rts. 6 (May 13, 2021), https://www.scribd.com/document/507913475/Apple-s-Senate-Subcommittee-Letter-May-2021 [https://perma.cc/BG76-TSFS] (writing that "privacy is a fundamental human right" and that the company designs all its products and services to be privacy-focused).

177. *See, e.g.*, Kate O'Flaherty, *Keeping iPhone Data Hidden from Apple Is 'Virtually Impossible,'* FORBES (Apr. 10, 2024, 6:41 AM), https://www.forbes.com/sites/kateoflahertyuk/2024/04/10/new-apple-iphone-privacy-warning-issued-by-researchers (on file with the *Iowa Law Review*) (discussing research); *see infra* note 316 and accompanying text.

178. *See Antitrust Applied: Examining Competition in App Stores*, *supra* note 171, at 10–11.

179. *See supra* Section I.A.2.ii.

180. *See, e.g.*, Comm'r of Competition v. Toronto Real Est. Bd., 2016 CT-2011-003, 76, 84 (Can.) (holding that the "principal motivation" for defendant's restriction on virtual office websites was "to insulate its [m]embers from the disruptive competition" and that privacy concerns were "an afterthought and continue to be a pretext"); *see also* Van Loo, *supra* note 52, at 103–06; Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 242–43 (2018); Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 837–39 (2019); Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 983–85 (2021).

A related but notably different factual scenario is the Google "Privacy Sandbox" initiative. Launched in 2019, the project was presented as an effort to devise new web standards that would improve user privacy while preserving advertising functionality. Mainly, Google sought to enable online advertising without the use of third-party cookies.[181] The project has progressed through several milestones, each drawing criticism for either insufficiently protecting user privacy, raising anticompetitive concerns, or both. Google's first major proposal, Federated Learning of Cohorts ("FLoC"), grouped users into cohorts based on browsing behavior for targeted advertising.[182] Although Google promoted FLoC as both effective and privacy preserving, it was quickly shown that it enabled new forms of tracking.[183] In addition, competition regulators expressed concern that FLoC would further entrench Google's market power.[184] FLoC's eventual replacement met similar criticism, and other proposals within the Privacy Sandbox framework have similarly been faulted for creating new privacy risks while simultaneously threatening to undermine competition in the online advertising ecosystem.[185] What is peculiar about the Privacy Sandbox case is that Google's conduct raised both privacy and competition concerns (almost as if there was an alignment between

181. Damien Geradin, Dimitrios Katsifis & Theano Karanikioti, *Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective,* 17 EUR. COMPETITION J. 617, 648–50 (2021) ("The Privacy Sandbox proposals are a series of browser Application Programming Interfaces (APIs) which would satisfy advertising use cases without relying on third-party cookies.").

182. *Id.* at 655–58.

183. *See, e.g.*, Bennett Cyphers, *Google's FLoC Is a Terrible Idea*, ELEC. FRONTIER FOUND. (Mar. 3, 2021), https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea [https://perma.cc/5U4P-9VL7] ("FLoC is meant to be a new way to make your browser do the profiling that third-party trackers used to do themselves: in this case, boiling down your recent browsing activity into a behavioral label, and then sharing it with websites and advertisers. The technology will avoid the privacy risks of third-party cookies, but it will create new ones in the process. It may also exacerbate many of the worst non-privacy problems with behavioral ads, including discrimination and predatory targeting.").

184. *See, e.g.*, Competition & Mkts. Auth., *Investigation into Google's 'Privacy Sandbox' Browser Changes*, GOV.UK (July 30, 2025), https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes [https://perma.cc/3AXE-9ZMF]; Foo Yun Chee, *Alphabet Hit with Austrian Privacy Complaint over Alleged Browser Tracking*, REUTERS (June 13, 2024, 3:37 PM), https://www.reuters.com/technology/alphabet-hit-with-austrian-privacy-complaint-over-alleged-browser-tracking-2024-06-13 [https://perma.cc/NB98-SZBQ].

185. *See, e.g.*, Rebecca Sentance, *Google's Privacy Sandbox: What Are the Latest Concerns?*, ECONSULTANCY (July 3, 2024), https://econsultancy.com/google-privacy-sandbox-concerns-third-party-cookies [https://perma.cc/3HPS-GHBJ]; Anthony Chavez, *Next Steps for Privacy Sandbox and Tracking Protections in Chrome*, PRIV. SANDBOX (Apr. 22, 2025), https://privacysandbox.com/news/privacy-sandbox-next-steps [https://perma.cc/KJX6-3JLH] ("[A] lot has changed since we announced the Privacy Sandbox initiative in 2019 and entered into a formal engagement with the CMA and ICO in 2022. For example, the adoption of privacy-enhancing technologies has accelerated, new opportunities to safeguard and secure people's browsing experiences with AI have emerged, and the regulatory landscape around the world has evolved considerably. Taking all of these factors into consideration, we've made the decision to maintain our current approach to offering users third-party cookie choice in Chrome . . . .").

them), but for separate unrelated reasons. Google supposedly meant to improve privacy in its surveillance operations but failed. The means by which it sought to achieve that happened to be also exclusionary and monopolistic, but not for the same reasons that Google's conduct undermined privacy.

The debate over whether improving the quality of services by means of increasing privacy protections might ever serve as a business justification for anticompetitive conduct remains contested.[186] It also serves as a source of conflict between those who would consider privacy as a component of quality cognizable to competition analysis at all, and those who would not.[187] These issues will likely be addressed further in the multiple cases recently brought by European regulators against Apple, Meta, and other big tech firms.[188]

Setting aside debates over the motivations of particular market actors in a given case, this discussion underscores the misalignment and the fundamental "trade-off" between competition and privacy, even when the latter is conceived as a component of quality or price.[189]

186. *See* Douglas, *The New Antitrust*, *supra* note 3, at 667 ("Antitrust analysis has not yet addressed whether user data privacy protection is cognizable as a business justification."). *But see* Epic Games, Inc. v. Apple, Inc., 67 F.4th 946, 986–88 (9th Cir. 2023) ("Epic's argument characterizes Apple as asserting security and privacy as independent justifications in and of themselves. But, throughout the record, Apple makes clear that by improving security and privacy features, it is tapping into consumer demand and differentiating its products from those of its competitors—goals that are plainly procompetitive rationales. . . . Apple's restrictions create a heterogenous market for app-transaction platforms which, as a result, increases interbrand competition—the primary goal of antitrust law. Antitrust law assumes that competition best allocates resources by allowing firms to compete on 'all elements of a bargain—quality, service, safety, and durability—and not just the immediate cost.' If we were to accept Epic and its *amici*'s argument, then no defendant could cite competing on non-price features as a procompetitive rationale." (citations omitted)).

187. *See* Douglas, *The New Antitrust*, *supra* note 3, at 667 (distinguishing between "Integrationist" theorists on the one hand, and "Separatist" theorists on the other).

188. *See, e.g.*, Press Release, Italian Competition Auth., A561-A561B - Italian Competition Authority: Investigation Opened Against Apple for Alleged Abuse of Dominant Position in the App Market (May 11, 2023), https://en.agcm.it/en/media/press-releases/2023/5/A561-A561B [https://perma.cc/6DLB-2XXH] (It.); Press Release, Bundeskartellamt, Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps (June 14, 2022), https://web.archive.org/web/20250330132449/https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html [https://perma.cc/K53G-PBHF] (Ger.); Press Release, UOKiK, Apple - The President of UOKiK Initiates an Investigation (Dec. 13, 2021), https://uokik.gov.pl/news.php?news_id=18092 [https://perma.cc/E6ZR-VFN8] (Pol.); Foo Yun Chee, *Exclusive: Meta Won't Tweak Pay-or-Consent Model Further Despite Risk of EU Fines, Sources Say*, REUTERS (July 11, 2025, 11:13 AM), https://www.reuters.com/sustainability/boards-policy-regulation/meta-wont-tweak-pay-or-consent-model-further-despite-risk-eu-fines-sources-say-2025-07-11 [https://perma.cc/7TEZ-KE53].

189. *See* Douglas, *The New Antitrust*, *supra* note 3, at 667 (discussing the trade-offs between competition and data privacy).

II. UNTANGLING ERRORS IN REGULATORY ANALYSIS: "PRIVACY" IN THE "MARKET"

There is no doubt that the market dominance of large data-intensive firms *both* creates structural impediments to competition by smaller entrants, and fuels extensive privacy-degrading surveillance. Yet, for the reasons discussed in Section I.A.2, competition law's focus on treating data as a business asset—aimed at creating and fostering competitive markets by increasing the number of firms engaged in data-extractive practices—often fundamentally conflicts with privacy objectives. After all, data extraction is in direct tension with the core aims of privacy protection.

Although in individual cases regulatory actions might incidentally affect privacy-increasing behaviors, as a general matter these regulatory approaches considering privacy as exogenous to competition will not, or at least not reliably, protect privacy.

Moreover, as discussed in Section I.B.2, considering privacy as a quality parameter often creates a head-to-head trade-off between competition and privacy concerns. From this vantage, data-protective practices may in and of themselves harm competition and reinforce market dominance.

The exercise of untangling privacy and competition concerns, however, pointed to two scenarios in which privacy and competition instincts do align. As discussed in Section I.A.1, the regulatory imposition of specific behavioral limits on data concentration and use by an individual firm, as in the case of the European Commission's review of the Google–Fitbit merger, can further both competition and privacy principles. And, as discussed in Section I.B.1, interests again strongly align in the case where consumers are locked into poor privacy conditions created by market-dominant firms unconstrained by meaningful competition.

As this Part discusses, however, even these arenas of conceptual alignment offer little real promise regarding the potential capacity of competition law to solve privacy law's problems. As an initial matter, the context in which regulators are comfortable addressing data concentration through behavioral restrictions that promote privacy has been limited, as it creates general dissonance with the notion that extra-competition considerations should not play a part in competition analysis. As articulated elsewhere by the FTC, "[n]ot only does the Commission lack legal authority to require conditions to [a] merger that do not relate to antitrust, [but] regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry."[190]

The notion that the lock-in phenomena will be solved by fostering competition over privacy, moreover, runs up against the real roadblocks to the development of such a market—and certainly a spontaneous one—well-

190. FTC, *supra* note 3, at 2.

established in the economic and legal literature.[191] These include the durable information asymmetry between firms and consumers, the costs of bargaining for the desired level of privacy, and the resulting "privacy paradox," which suggests that, despite consistently expressing strong preferences for privacy, people often behave in ways that ultimately align with or enable surveillance.[192]

More fundamentally, although our analysis identifies two instances where privacy and competition concerns theoretically align, this Part shows that any such alignment is profoundly undermined by two pervasive analytic errors in regulatory analysis made by regulators, courts, and commentators. These errors lead to outcomes that undermine privacy, even in cases where privacy and competition interests appear aligned.

The first error in the analysis of privacy is a fundamental misconception of privacy in relation to markets: conceiving it too narrowly, perceiving it as exogenous to market dynamics, and failing to recognize privacy's compelling interest in the reduction of behaviors that facilitate surveillance. The second is an error in the analysis of markets. This error is compound. First, it reflects the reality that competition analysis legitimizes and prioritizes surveillance and predictive behavior markets through an agnosticism regarding the substance of the markets in which it seeks to promote innovation, competition, and growth. Second, having done that, the analysis in recent competition cases has been strikingly slippery in articulating the relevant markets; it confuses and conflates, on the one hand, markets in which privacy is a good that can be the subject of potential competition, i.e., consumer markets, and on the other, markets where privacy is at best insignificant and at worst a roadblock to competition, i.e., surveillance markets.

Together, these errors form the foundation of an anti-privacy framework leading to three key consequences: (1) where privacy and competition conflict, the thin understanding of privacy will never win against the agnostic promotion of competition; (2) it seems unlikely that competition will rarely, if ever, facilitate the creation of markets for privacy to address concerns like lock-in; and (3) competition will not offer tools to address firms' use of markets to engage in the most comprehensive of privacy-injuring practices—surveillance markets. Competition law then, will just tinker around the edges. Thus, even in scenarios where privacy and competition concerns might theoretically align, the net outcome for privacy will be deleterious.

A. THE FIRST ERROR: MISCONCEIVING "PRIVACY"

In the first type of error, competition regulators underestimate the significance of the right to privacy or misinterpret its content, revealing a lack

191. *See, e.g.*, Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3, 4–8 (1997).

192. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 48–49 (2021) (describing reasons why it is rational for people to fail to make good assessments of privacy risks and to fail to manage their privacy effectively).

of understanding of its full scope and purpose. They often treat privacy as a thin concept reduced to narrow issues like data security, consent, or consumer choice. Even these limited dimensions of privacy are interpreted superficially, with regulators frequently regarding privacy merely as an intermediate value or goal intended to serve broader economic protections, rather than as a fundamental right in and of itself.

To be clear, we are not the first (to say the least) to point out that privacy does not—and should not—equal either "consent," "control," and "choice," or data security.[193] In fact, the centrality of consent, control, and choice to privacy regulation has been criticized by many and often, on theoretical, analytical, and empirical grounds.[194] And although regulators typically seem to believe in the general desirability of privacy consent and data control rights, scholars have warned against the fixation on these mechanisms and the tunnel vision they produce with negative effects on privacy laws.[195]

Our critique of regulators is twofold. First, they have not internalized the ongoing discussions in privacy literature and by researchers in the field about the complete failure of privacy consent, control, and choice. Second, and separately, they have construed privacy interests in a cramped and superficial way, devaluing and deprioritizing it in ways that privilege the promotion of systemic surveillance.

---

193. *See, e.g.*, ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 45–46 (2021).

194. *See, e.g.*, Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 604 (2024) ("Severe deficiencies in consent are papered over with one fiction after another."); Corren, *supra* note 79, at 2021; Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 555–60 (2023); Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1272 (2022) (critiquing the "theory of privacy-as-control embedded in the rights/compliance model" as "habituat[ing] us into a false sense of control while technology companies weaponize our exercise of individual rights to immunize themselves from legal accountability"); JULIE E. COHEN, HOW (NOT) TO WRITE A PRIVACY LAW 5 (2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/A2MT-QCB8]; JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 262–63 (2019); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426–31 (2018); *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 69–71 (2018) (critiquing the approach to privacy law that is focused solely on the individual and emphasizing privacy's social and collective values); NEIL RICHARDS, WHY PRIVACY MATTERS 38–39 (2022) (developing a theory of privacy as rules). For earlier critiques, see, for example, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013); Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 862 (2000); and Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1660–64 (1999).

195. *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 21–22 (2015) (describing how the focus on these approaches "reduce privacy protection to an individual right to 'a procedural order, not a substantive guarantee: if the rules are followed (consent forms, warrants, boilerplate notifications) then the objections are null'" (quoting John Gilliom, *A Response to Bennett's 'In Defence of Privacy,'* 8 SURVEILLANCE & SOC'Y 500, 504 (2011))).

Our central unit of analysis is the position of competition regulators on issues of privacy, though admittedly our critique of the narrow conception of privacy also reaches the frameworks embraced by privacy regulators and privacy law. Although a fuller account of privacy as freedom from surveillance is developed elsewhere,[196] this Section shows that when privacy is reduced to an overly thin and superficial notion in the context of "the market," the result is serious analytical and regulatory shortcomings that prevent any real control over the conduct of powerful market actors.

1. The Challenging Economic Analysis of Privacy

One of the persistent complexities of privacy law is its inherent vagueness. What is privacy? How should it be defined, and based on that definition, how should it be protected? In the privacy theory literature, these questions have become almost a cliché, yet they remain open. Various definitional paths have been suggested, and scholars have attributed the failures of socio-legal privacy frameworks to this lack of resolution.[197]

Traditionally, the definitional discussions within privacy theory have been philosophical and normative, and non-economic, thus not situating "privacy" in the market (or assuming it is fulfilling a market function). However, there is a growing trend of analyzing privacy using economic tools.[198] Unsurprisingly, the economic analysis of privacy too is fraught with uncertainties, much like the general literature on privacy theory.

The privacy economics literature includes several prominent perspectives. One such perspective views privacy as the concealment of information, a concept dating back to the 1970s. As the free flow of information is assumed to be fundamental to the proper functioning of markets, this view suggests that information facilitates market efficiencies. Conversely, privacy, by limiting the availability of information, can potentially create inefficiencies by denying relevant information from market participants.[199]

---

196. *See generally* Bamberger & Corren, *supra* note 16.

197. *See, e.g.*, sources cited *supra* notes 193–94; Deirdre K. Mulligan, Colin Koopman & Nick Doty, *Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, PHIL. TRANSACTIONS ROYAL SOC'Y A 3 (Dec. 28, 2016), https://www-jstor-org.proxy.lib.uiowa.edu/stable/26115828?seq=1 (on file with the *Iowa Law Review*); María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 509–11 (2024); Salomé Viljoen, *The Broader Lessons of Privacy Law*, 104 B.U. L. REV. 1131, 1135 (2024).

198. Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 443 (2016).

199. *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394–95 (1978); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 406 (1981); Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817, 1834–35 n.36 (1993); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 633–34 (1980).

A countervailing account understands privacy and surveillance to implicate a multiplicity of diverse economic trade-offs that are hard to resolve unless we account for specific context.[200] Thus, on the one hand, the privacy of personal information can yield economic gains for individuals. For example, privacy protections may prevent a firm from engaging in price discrimination by concealing a consumer's reservation price (i.e., the maximum price that they are willing to pay).[201] Yet on the other hand, some degree of surveillance can also benefit individuals. For example, a consumer may experience reduced search costs and increased accuracy of search results when using a search engine that closely tracks their online activity.[202] Additionally, to complicate matters, the trade-offs created by privacy and surveillance exist not only at the individual level, but they manifest at the collective level as well, as both positive and negative externalities. For instance, society as a whole may enjoy *benefits* that arise from surveillance, such as those that come from collecting and analyzing personal health information and consequently arriving at new medical knowledge.[203] On the other hand, society as a whole may suffer *harms* that arise from surveillance, such as those that come from over-policing citizens, limiting their choices, or chilling their speech.[204]

Furthermore, the entire notion of how to even measure economic trade-offs between privacy and surveillance implicates complications arising from unique characteristics.[205] For example, these trade-offs are intertemporal, meaning that while forgoing one's privacy in a commercial setting often provides an immediate benefit, the costs of doing so are uncertain both in amount (how much one will pay for their exposure) and in timing (when one will pay). Privacy/surveillance trade-offs also tend to mingle the tangible (price), with the intangible (autonomy harm from having to reveal one's personal information), with the incommensurable (surveillance's effect on society as a whole).[206]

Complexity arises not only from the incommensurability of the trade-offs between the costs and benefits of surveillance, but from the diverging accounts of privacy's value when analyzed directly as an economic good. One reason is that information, including personal information, has the characteristics of a public good (i.e., being nonrivalrous and nonexcludable), and yet privacy protections are all about excluding firms, the government, and others from knowing personal information.[207] Another reason is that the

200. Acquisti et al., *supra* note 198, at 443–44.

201. *Id.* at 445.

202. *Id.*

203. *Id.*

204. *Id.* at 446.

205. *Id.* at 446–48.

206. *Id.* at 447.

207. *Id.* at 446; *see also* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 442–43 (2015). *But see* Ayelet Gordon-Tapiero, Katrina Ligett & Kobbi Nissim, *On*

value of privacy for a certain piece of personal information is highly context-dependent (people compartmentalize and share or suppress different pieces of information with different audiences for various purposes),[208] and it is also contingent on specific and idiosyncratic individual privacy sensitivities and attitudes. The value of information may also change over time.[209] A third reason is that privacy may be seen both as a final good—a good with intrinsic value for consumers—but also as an intermediate good—a good that is valued for instrumental purposes.[210]

It is no wonder then that competition regulators in particular have struggled with defining privacy when addressing anticompetitive behavior in digital markets. And too often they seem to have gotten it wrong.

2. Errors in Framing Privacy: Privacy Is Not (Only) Consent, Control, and Consumer Choice

The European Commission—the primary competition law regulator in the European Union—tends to cabin privacy's meaning within a consumer choice rubric. One example is the Facebook–WhatsApp merger from 2014. The European Commission did not dedicate much of its analysis to the privacy implications of the merger. When it did consider privacy, however, it briefly treated it as a product feature that may appeal to some consumers more than to others (i.e., a consumer preference).[211] It explicitly declared that "[a]ny 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 E.U. competition law rules but within the scope of the E.U. data protection rules."[212] Thus, it considered privacy as a possible consumer preference—but in the end not even one economically important enough to justify an evaluation of market impact. When it was revealed in 2016 that

the Rival Nature of Data: Tech and Policy Implications, 2025 PROC. SYMP. ON COMPUT. SCI. & L. 17–18, https://dl.acm.org/doi/abs/10.1145/3709025.3712211 [https://perma.cc/P5GJ-AEVZ] (arguing that privacy concerns can make data rivalrous).

208. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129–58 (2009); Acquisiti et al., *supra* note 198, at 446 ("The value of keeping some personal information protected and the value of it being known are almost entirely context-dependent and contingent on essentially uncertain combinations of states of the world.").

209. Acquisti et al., *supra* note 198, at 446–47.

210. *Id.* at 447.

211. FACEBOOK/WHATSAPP EC MERGER REVIEW, *supra* note 39, ¶¶ 86–87, 102, 173–79; *see also* Orla Lynskey, *Considering Data Protection in Merger Control Proceedings* 7 (Org. for Econ. Coop. & Dev., Working Paper No. JT03465800, 2018) ("[I]n *Facebook/Whatsapp* the Commission did not interrogate the conclusion that competition on the basis of data protection does not yet exist, assuming that markets involving personal data function efficiently and reflect consumer preferences.").

212. FACEBOOK/WHATSAPP EC MERGER REVIEW, *supra* note 39, ¶ 164; *see also* Lynskey, *supra* note 211, at 10 ("In light of the complex economic, social and political ramifications of personal data aggregation, a more cautious approach to data-driven mergers might be advised. At its most extreme, this would amount to a moratorium on acquisitions by certain companies . . . .").

Facebook had knowingly misled the regulator on a privacy issue that was part of the European Commission's merger review investigation, the European Commission slapped Facebook on the wrist with a fine but did not reopen its decision.[213] This is perhaps unsurprising, as the European Commission's 2014 decision explicitly noted that this specific privacy issue—even if Facebook had not (misleadingly) claimed it was resolved—would not have been significant enough to affect its approval of the merger.[214]

As discussed above,[215] the FTC similarly approved the Facebook–WhatsApp merger while highlighting the privacy "promises" and thus obligations of both firms, focusing on what users "understand[]" and what they have "consent[ed]" to.[216] The FTC also noted that if these privacy promises were not honored post-merger, both firms could be found in violation of Section 5 of the FTC Act for deceptive and unfair practices.[217] The FTC did not follow through on this promise,[218] though it did regret the merger.[219]

The European Commission again framed privacy in a cramped way, as a consumer choice technicality, in its 2016 merger review of the Microsoft–LinkedIn deal. This time, the European Commission did broaden its perspective to include privacy as "an important parameter of competition"[220] that justifies market evaluation, but still treated it as a superficial and procedural matter. The European Commission raised the possibility that "foreclosure effects would lead to the marginalisation of an existing competitor which offers a greater degree of privacy protection to users than LinkedIn (or make the entry of any such competitor more difficult)."[221] In raising concerns about

213. After the Facebook/WhatsApp merger was complete, the European Commission discovered that Facebook misrepresented privacy aspects of the deal; it told the European Commission that it would not be able to match Facebook user accounts to the phone numbers of WhatsApp users, but it was revealed otherwise when in 2016 Facebook updated WhatsApp terms to allow it to do exactly such matching. After the European Commission investigated further, it was revealed that the technical feasibility to do such matching already existed in 2014, and Facebook was aware of it and knowingly misled the regulator. *See* European Commission Press Release IP/17/1369, *supra* note 40.

214. *See* FACEBOOK/WHATSAPP EC MERGER REVIEW, *supra* note 39, ¶¶ 185–89.

215. *See supra* notes 39–43 and accompanying text.

216. Letter from Jessica L. Rich, *supra* note 42, at 1–2 (after citing from WhatsApp's privacy policy on the centrality of user consent to users' privacy, noting that "WhatsApp's hundreds of millions of users have agreed to use the WhatsApp service, and to have WhatsApp collect and transmit their information, with the understanding that these promises will be honored"); *see also* Press Release, FTC, *supra* note 41.

217. Letter from Jessica L. Rich, *supra* note 42, at 3.

218. The FTC did not take action similar to the European Commission after it was revealed that Facebook misled regulators about maintaining users' privacy post-merger. *See supra* notes 39, 207–08, and accompanying text.

219. *See supra* notes 139–43, *infra* notes 245–46, and accompanying text (discussing the FTC's federal lawsuit against Facebook (now Meta) for the monopolization of the personal social networking market by, inter alia, buying Instagram and WhatsApp).

220. MICROSOFT/LINKEDIN EC MERGER REVIEW, *supra* note 137, ¶ 350 n.330.

221. *Id.*

post-merger foreclosure effects, the European Commission also identified a concrete example of such a competitor, a similar platform called Xing that at that time was perceived to provide greater privacy than LinkedIn.

The European Commission's discussion of Xing highlights the limited understanding of "privacy" the European Commission had in mind. Xing[222] offered "better" privacy, they argued, because the platform "ask[ed] users to actively accept [its] privacy policy . . . by ticking a box, whereas LinkedIn users accept LinkedIn's privacy policy automatically when they press the button 'join now.'"[223] This illustrates the European Commission's reliance on a highly formalistic interpretation of consent, assuming that the act of ticking a box in one context versus another constitutes an effective means of safeguarding privacy. However, not only are both acts of ticking a box functionally equivalent, but they are also equally ineffective at ensuring meaningful consent.[224] Additionally, when the competing app made a change that had privacy implications, it sought active user consent while LinkedIn did not, and regardless of whether such consent was given, users did not lose functionality.[225] Although this policy is commendable, the literature repeatedly shows that the opt-in privacy consent model often offers a poor means for achieving real consent, making this a distinction without a difference.[226] Importantly, under this approach, privacy is no more than a technical feature that some consumers may click on or toggle while others may not. For example, there is a complete disregard to the fact that any firm—LinkedIn or its competitors—might change its privacy policy and privacy settings at any time, whether or not consumers are happy about it or agree to it.[227] Even though the European Commission considered the risk that privacy would be marginalized post-merger, it nevertheless approved the merger subject to commitments offered by Microsoft.[228]

Highlighting the lack of attention by competition regulators to privacy and its market implications, the 2011 Microsoft–Skype merger—despite

222. *Id.* ("By way of example, the results of the Commission's investigation revealed that, today, in Germany and Austria, Xing seems to offer a greater degree of privacy protection than LinkedIn.").

223. *Id.*

224. *See* Corren, *supra* note 194, at 564–66, 575–76.

225. MICROSOFT/LINKEDIN EC MERGER REVIEW, note 137, ¶ 350.

226. *See* Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155, 1200–10 (2013).

227. MICROSOFT/LINKEDIN EC MERGER REVIEW, *supra* note 137, ¶ 350; Srinivasan, *supra* note 114, at 69–71.

228. Including that Microsoft will not tie LinkedIn to Windows, will allow rivals certain interoperability with Microsoft Office, and will grant software developers access to certain tools. European Commission Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_16_4284/IP_16_4284_EN.pdf [https://perma.cc/XM2P-G7XR].

being similar in nature to the Facebook–WhatsApp deal—did not raise any privacy concerns with the European Commission.[229] The 2012 deal for the purchase of Instagram by Facebook was not even investigated by the European Commission.[230]

Tracking the European Commission, the FTC in real time had sidestepped Facebook's buying-the-competition spree. In laconic identical letters to the counsels of Facebook and Instagram, in 2012 the FTC announced that after conducting an antitrust investigation, "no further action is warranted by the Commission at this time. Accordingly, the investigation has been closed."[231]

Recently, privacy consent has been directly integrated into E.U. competition law. When the German Facebook case was decided in July 2023 by the CJEU, the court addressed several novel issues. The primary one, as discussed above,[232] was whether a competition authority investigating an abuse of dominance could consider unlawful behavior under privacy law, such as the GDPR.[233]

Another was whether consent can be "freely given" when obtained by a dominant firm.[234] The CJEU held that dominance "does not, as such, preclude" valid consent, but clarified that dominance is "an important factor" in assessing whether consent is in fact free, which the firm must prove.[235] This is because market dominance "is liable to affect the freedom of choice of . . . user[s], who might be unable to refuse or withdraw consent without detriment,"[236] and "may create a clear imbalance . . . between the data subject

229. *See generally* EUR. COMM'N, CASE NO COMP/M.6281 – MICROSOFT/SKYPE (Oct. 7, 2011), https://ec.europa.eu/competition/mergers/cases/decisions/m6281_924_2.pdf [https://perma.cc/VR98-N5A5] (does not mention "privacy").

230. It was reviewed by the United Kingdom's Office of Fair Trading and by the FTC, and both cleared the deal. *See* OFF. OF FAIR TRADING, No. ME/5525/12, ANTICIPATED ACQUISITION BY FACEBOOK INC. OF INSTAGRAM INC. 10 (Aug. 22, 2012), https://assets.publishing.service.gov.uk/media/555de2e5ed915d7ae200003b/facebook.pdf [https://perma.cc/JD6Z-UUNP]; Press Release, FTC, FTC Closes Its Investigation into Facebook's Proposed Acquisition of Instagram Photo Sharing Program (Aug. 22, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition-instagram-photo-sharing-program [https://perma.cc/B5G8-UK92].

231. Letter from April J. Tabor, Acting Sec'y, FTC, to Thomas O. Barnett, Esq., Covington & Burling LLP (Aug. 22, 2012), https://www.ftc.gov/sites/default/files/documents/closing_letters/facebook-inc./instagram-inc./120822barnettfacebookcltr.pdf [https://perma.cc/MY26-832D] (writing to Facebook's attorney that "no further action is warranted" by the FTC); Letter from April J. Tabor, Acting Sec'y, FTC, to Patricia R. Zeigler, Esq., Orrick, Herrington & Sutcliffe LLP (Aug. 22, 2012), https://www.ftc.gov/sites/default/files/documents/closing_letters/facebook-inc./instagram-inc./120822zeiglerinstagramcltr.pdf [https://perma.cc/WRJ2-NBVD] (communicating the same to Instagram's attorney).

232. *See supra* notes 44–46 and accompanying text.

233. Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, ECLI:EU:C:2023:537, ¶¶ 36–63 (July 4, 2023).

234. *Id.* ¶ 140.

235. *Id.* ¶ 154.

236. *Id.* ¶ 148 (referring to Council Regulation 2016/679, 2016 O.J. (L 119) recital 42).

and the controller."[237] The court further noted that where data processing is not necessary for the performance of a contract,[238] users must be offered granular choices enabling refusal "without being obliged to refrain entirely from using the service . . . which means [they] are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations."[239]

Thus, although versions of pay-or-consent existed beforehand, the CJEU decision made it a central solution for firms like Meta: Simple one-stop-shop consent was no longer acceptable, yet targeted advertising had to continue. In November 2023, Meta introduced its model requiring users either to consent to its privacy-invasive behavioral advertising, or pay a monthly fee for Instagram and Facebook.[240] This attracted immediate scrutiny. The European Data Protection Board ("EDPB") opined that such a binary model generally violates GDPR consent requirements, emphasizing that a dominant firm must also offer an "equivalent alternative" without a fee (e.g., based on non-behavioral advertising).[241] In April 2025, the European Commission found Meta in breach of the DMA for related reasons and fined it €200 million.[242] Under the DMA, gatekeepers must obtain GDPR-standard user consent for combining personal data between services, and users who decline "must have access to a less personalised but equivalent alternative."[243] The European Commission found Meta's original binary pay-or-consent model in violation of the DMA as it only introduced "a choice between consenting to personal data combination for personalised advertising or paying a monthly subscription for an ad-free service," and "did not give users the required specific choice to opt for a service that uses less of their personal data but is otherwise equivalent to the 'personalised ads' service."[244]

Multiple regulators and courts thus ultimately reached this set of outcomes all centered on consent. In practice, this means you can pay for privacy with money ("pay"), you can pay for products and services with your privacy ("consent"), or you can accept reduced quality as the price of privacy (an

237. *Id.* ¶ 149 (referring to Council Regulation 2016/679, recital 43 & art. 7(4) 2016 O.J. (L 119)).

238. *Id.*

239. *Id.* ¶ 150.

240. *EDPB Opinion: Meta Cannot Rely on "Pay or Okay,"* NOYB (Apr. 17, 2024), https://noyb.eu/en/statement-edpb-pay-or-okay-opinion [https://perma.cc/9W5S-VF7F].

241. EDPB, OPINION 08/2024 ON VALID CONSENT IN THE CONTEXT OF CONSENT OR PAY MODELS IMPLEMENTED BY LARGE ONLINE PLATFORMS 39–40 (Apr. 17, 2024), https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf [https://perma.cc/H9JQ-D7P5].

242. European Commission Press Release IP/25/1085, Commission Finds Apple and Meta in Breach of the Digital Markets Act (Apr. 23, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085 [https://perma.cc/7ZF6-6RFN].

243. *Id.*; *see also* Council Regulation 2022/1925, art. 5(2) 2022 O.J. (L266).

244. European Commission Press Release IP/25/1085, *supra* note 242.

"equivalent alternative").[245] The DMA itself permits a degradation in quality where it "is a direct consequence of the gatekeeper not being able to process such personal data"[246]—a justification likely to be invoked frequently.

This approach puts privacy on a continuum of "quality" that tracks across jurisdictions. It implicates the privacy lock-in scenario, where privacy and competition arguments supposedly align.[247] But it gets confused because "quality" can stand for anti-privacy dimensions as well.

In 2020, eight years after Facebook bought Instagram and six years after it bought WhatsApp, the FTC changed its mind and brought suit against Facebook alleging that it has monopolized the personal social networking market by, among other things, buying Instagram and WhatsApp.[248] As noted above, in its complaint the FTC discusses a privacy-as-quality parameter that Facebook deteriorated once it had market power.[249] The privacy-as-quality approach was also adopted by the DOJ in its 2020 case against Google for monopolizing online search markets.[250] In its complaint, the DOJ argued that "[b]y restricting competition . . . 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), lessening choice . . . and impeding innovation."[251] Expanding on harms to innovation, the DOJ added:

> Google's grip over distribution also thwarts potential innovation . . . . [O]ne company recently started a subscription-based general search engine that does not rely on advertising profits derived from monetizing user information. Another, DuckDuckGo, differentiates itself from Google through its privacy-protective policies. But Google's control of search access points means that these new search models are denied the tools to become true rivals . . . .[252]

Even when considered as a quality parameter, privacy is still narrowly framed within a consumer choice and consent rubric—a framework easily eclipsed by broader economic and business considerations. In this framing, privacy-as-quality is often cast against other, ostensibly more "important"

---

245. *See generally* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369 (2017) (examining the different ways companies handle data privacy).

246. Council Regulation 2022/1925, 2022 O.J. (L 265) recital 37; *see also id.* at recital 36.

247. *See supra* Section II.B.1.

248. *See supra* notes 138–43 and accompanying text.

249. FTC 2021 Facebook Complaint, *supra* note 142, ¶ 163.

250. Amended Complaint at 2, United States v. Google LLC, 747 F. Supp. 3d 1 (D.D.C. 2024) (No. 20-cv-3010) ("The United States of America . . . bring this action under Section 2 of the Sherman Act, 15 U.S.C. § 2, to restrain Google LLC (Google) from unlawfully maintaining monopolies in the markets for general search services, search advertising, and general search text advertising in the United States through anticompetitive and exclusionary practices, and to remedy the effects of this conduct.").

251. *Id.* at 53.

252. *Id.* at 5.

dimensions of quality. In August 2024, the court in the Google search monopolization case ruled that "Google is a monopolist, and it has acted as one to maintain its monopoly."[253] The court's detailed decision shows how the entire industry perceives privacy as a trade-off with quality and/or profits. It notes, for example, that Google recognized users' growing concern for privacy,[254] and at times considered "undertaking privacy initiatives after looking to rivals," but ultimately weighed these against "the business case for making privacy-focused changes"[255] (i.e., the lack thereof). Citing Google's Senior Vice President of Knowledge and Information Products, the court reveals that Google's stance was "that merely because 'people care increasingly about privacy' and '[DuckDuckGo] is making a lot [of] noise about it,' it did not mean that Google needed 'a product change.'"[256] As he put it: "[M]y pushback was maybe we do, maybe we don't, but I'd like to see the data on the impact on users, and on our ability to build a good search and search ad system."[257] The court aptly summarized Google's view as "a trade-off between *search quality* and user privacy."[258] It then compared Google's surveillance and privacy choices to DuckDuckGo's, underscoring Google's systemic anti-privacy approach.[259] At other points, the court showed how privacy was treated as directly undermining business operations, firm profit, or the quality of Google's ad targeting.[260]

---

253. *Google LLC*, 747 F. Supp. 3d at 32.

254. *Id.* at 54.

255. *Id.* at 54–55.

256. *Id.* at 55.

257. *Id.*

258. *Id.* (emphasis added) (the court further cites Google's Senior Vice President, Knowledge and Information Products as "agreeing that an incognito mode feature could be accomplished '[a]s a technical matter,' but '[t]hat doesn't make a good product design'" and noting that "[DuckDuckGo] might also not be the best model for Google users' privacy needs").

259. *Id.* at 55–56 ("The degree of privacy a [general search engine] offers reflects a series of individual design decisions. Whether to track a user's sessions data is one such decision. According to Google, tracking user sessions is 'measurably beneficial to the user experience, including things like []in-session use of context to improve results.' Such data also helps to tailor the advertisements that Google delivers to a user. [DuckDuckGo], on the other hand, anonymizes user click data and does not track user sessions. It therefore cannot discern whether multiple searches are the same user performing different actions. How a [general search engine] uses IP addresses is another design decision. Google logs IP addresses and uses them to customize search results. [DuckDuckGo], in contrast, does not log IP addresses. . . . Google also logs IP addresses to enhance security. [DuckDuckGo] 'had developed [its] own click fraud systems' that do not require logging of IP addresses. Another question of privacy design is whether to invite users to 'sign in.' Google does so because it believes such functionality improves search results and overall search engine quality. [DuckDuckGo] does not have an option for users to 'sign in' to its platform. How much user data a [general search engine] retains also is a measure of privacy. Google chose to retain 18 months, even though some survey data suggested users preferred a shorter retention period. The decision to retain 18 months of a user's data versus fewer months was largely arbitrary." (citations omitted)).

260. *Id.* at 70 ("Privacy initiatives can also limit the effectiveness of . . . targeting techniques. Retargeting data is collected using 'cookies' or data about an individual's prior web activity

Ultimately, the court too adopts the privacy–quality trade-off truism, and therefore disagreed with the government's claim that Google's conduct reduced the quality of search services along the privacy dimension, and that "Google's ability to offer fewer privacy protections—without concern as to a rival's superior privacy offerings—is evidence of monopoly power."[261] The court found that "using privacy to demonstrate monopoly power is questionable," and that "[p]laintiffs have not established any framework for evaluating whether Google's privacy offerings are suboptimal"[262]—a surprising remark given the court's own analysis of Google's consistent anti-privacy design choices. The court also found little "proof of monopoly power [in] that Google considers the business case for making privacy adjustments," as "[t]here is some tradeoff between privacy and search quality. . . . That Google offers fewer privacy protections than [DuckDuckGo] without losing users is thus not necessarily indicative of monopoly power. It may just be that users are willing to sacrifice enhanced privacy offerings for improved search functionality."[263]

Taken together with the Google court's reasoning, the effect is to treat privacy as a fungible commodity, traded off against money or other dimensions of quality. Even where regulators and courts claim to weigh both privacy and competition, the outcome mirrors the Google court's logic: privacy is consistently subordinated. Once consent is the operative mechanism, the supposed "choices" collapse into the same set of trade-offs—surrender data, pay more, or accept diminished service quality. In markets dominated by powerful gatekeepers, each path reinforces the erosion of privacy rather than its protection.[264]

. . . . Cookies can be limited by third parties. For instance, after Apple made privacy changes to a new version of iOS, Meta's ability to serve retargeting ads was made 'much harder or potentially even not possible in some circumstances.'"); *id.* at 74–75 (when discussing "metrics advertisers use to evaluate the effectiveness of their ad spend," such as "return on investment (ROI), or return on ad spend (ROAS)," the court notes that "it is challenging for advertisers to calculate ROI and ROAS. . . . [P]rivacy measures have made it 'more challenging for [JPMorgan Chase's] teams to have real-time access to performance data at a granular level'" (citations omitted)); *id.* at 84 ("Prior to 2020, [search query reports] included all queries that resulted in an ad click, even if there was only a single click (i.e., the 'one-click threshold'). Ostensibly out of privacy concerns, Google removed the one-click threshold. It did so notwithstanding 'substantial' projected data loss for advertisers and knowing that specific major advertisers . . . had stated they would be harmed." (citations omitted)).

261. *Id.* at 119–20; *see supra* notes 122–27 and accompanying text.

262. *Google LLC*, 747 F. Supp. 3d at 118.

263. *Id.* at 119; *see also* Saladrigas et al., *supra* note 63 ("The court spent considerable time analyzing the evidence around Google's privacy practices in these markets, including the potential negative downstream impacts related to consumer privacy, as well as the failed attempts at privacy-focused innovation in these markets. Nevertheless, the court ultimately refused to consider privacy in its assessment of monopoly power.").

264. Another recent example for how firms use consent to evade liability for surveillance is *Calhoun v. Google LLC*, 113 F.4th 1141, 1147–48 (9th Cir. 2024) (the court treats privacy consent as real, literal consent, which hurts the ability of a group to sue Google for collecting personal data

As noted earlier, there is a well-established critique of the notion that privacy is exclusively or primarily about consent, control, and choice.[265] Relying on consent, control, and choice as the mechanism for regulating the production and distribution of privacy is fraught with issues—including severe information asymmetries between individuals and firms, manipulative design and dark patterns, intentionally manufactured complexity, proceduralism instead of substance, and the limits of human rationality and attention spans. Time and again, consent-based frameworks have demonstrably failed. Thus, the cramped construction of privacy often adopted by regulators ignores a vast body of research demonstrating that people are unable to exercise their theoretical consent, control, and choice as real power or as a genuine expression of autonomy against firms in the surveillance economy.

3. Errors in Framing Privacy: Privacy Is Not (Only) Instrumental to Other Values

Another problematic understanding of privacy that is different but equally limited considers privacy to be a servant of other master goals—a mere instrument for achieving other objectives, failing to recognize privacy's intrinsic value. Competition regulators have at times treated privacy as a means to mitigate economic and other non-privacy-related harms, with privacy itself being a secondary concern rather than a fundamental right or an independent concern worthy of protection. In that context, privacy is often depicted as a means to promote competition and fairness in consumer marketplaces rather than an end of itself or a good over which competition should exist.[266]

This approach has been typical for the FTC. For example, a former director of the FTC's Bureau of Consumer Protection, Jessica Rich, highlighted in 2014 that big data poses significant problems beyond lacking consent and deficient security.[267] More critically, it can adversely affect access to "credit, insurance, employment or other benefits."[268] Rich also raised concerns that firms will use big data to price discriminate against vulnerable populations.[269]

---

even when users specifically chose not to sync their Chrome browsers with their Google accounts). *See also* Yafit Lev-Aretz, *Clicking 'I Agree' Online Lets Data In and Keeps Lawyers Out*, HILL (July 22, 2025, 10:30 AM), https://thehill.com/opinion/technology/5412603-clicking-i-agree-onlineshouldnt-void-your-privacy-rights [https://perma.cc/KWP2-U45B].

265. *See supra* notes 187–89 and accompanying text.

266. *See* Acquisti et al., *supra* note 198, at 447.

267. Letter from Jessica L. Rich, Dir., Bureau of Consumer Prot., to Nat'l Telecomms. & Info. Admin. 7 (Aug. 1, 2014) [hereinafter FTC Rich Comment 2014], https://www.ftc.gov/system/files/documents/public_statements/573301/140801bigdatacomment.pdf [https://perma.cc/YN8T-27EH].

268. *Id.* Rich highlighted how troves of personal information can be used to infer other sensitive information ("ethnicity, income, religion, political leanings, age, and health conditions"). *Id.*

269. *Id.* at 8 ("Speakers at our seminar also raised concerns about the use of Big Data to engage in price discrimination. While some stated that competition could resolve consumer concerns regarding dynamic pricing, others expressed concern that consumers in lower-income

This discussion underscored the perspective that privacy protections are not a primary concern, but they should be employed to prevent economic harms resulting from firms' discrimination based on personal data.

Similarly, a 2016 FTC report examined the "impact of big data on low-income and underserved populations."[270] The report highlighted concerns about inaccuracies and biases in personal data that could negatively impact the availability of products and services to these groups.[271] Examples included "individuals mistakenly being denied opportunities based on the actions of others" with shared characteristics,[272] "creat[ing] or reinforc[ing] existing disparities" by using personal data to target ads to certain populations and not others,[273] and offering "higher-priced goods and services for lower income communities."[274] The common thread among these and other concerns was that "big data offers companies the opportunity to facilitate [economic] inclusion or exclusion."[275] As the report notes, there is no question as to *whether* firms will use big data and surveil consumers in the process—of course they will. The important question to answer is *how* firms will use personal data and its analytics.[276]

Another example of the approach that utilizes privacy to advance economic goals is the 2019 action in the matter of Google and YouTube.[277] The FTC together with the State of New York found Google and YouTube to have extensively violated the Children's Online Privacy Protection Rule.[278] They reached a settlement that included a $170 million penalty alongside

---

neighborhoods without competition from brick-and-mortar stores would be charged higher prices. We intend to explore these issues further . . . ." (footnotes omitted)).

270. *See* FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 2–3 (2016) [hereinafter FTC 2016 REPORT], https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/3W79-AXCH].

271. *Id.* at 8; *cf. id.* at A-1 (Commissioner Maureen K. Ohlhausen stating in a separate statement that there are concerns about inaccuracies and biases in personal data).

272. *Id.* at 9.

273. *Id.* at 10.

274. *Id.* at 11.

275. *Id.* at 12.

276. *Id.*; *see also id.* at 21–23.

277. *See* Press Release, FTC, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/4R5U-K9LJ].

278. FTC, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA *IN THE MATTER OF GOOGLE LLC AND YOUTUBE, LLC* 1 (2019) [hereinafter CHOPRA GOOGLE DISSENT], https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf [https://perma.cc/R2QK-MWYS] ("For the third time since 2011, the Federal Trade Commission is sanctioning Google for privacy violations. This latest violation is extremely serious. The company baited children using nursery rhymes, cartoons, and other kid-directed content on curated YouTube channels to feed its massively profitable behavioral advertising business.").

conduct relief.[279] Dissenting from the settlement, former Commissioner Chopra criticized what he characterized as "insufficient remedies to address the company's financial incentives, and a fine that still allows the company to profit from its lawbreaking," concluding that "[t]he terms of the settlement were not even significant enough to make Google issue a warning to its investors."[280] Importantly, Commissioner Chopra argued that both Google and YouTube's wide-ranging *privacy* violations further entrench Google's *dominance* in digital markets and the information economy broadly speaking.[281] The argument's logic was that more information collected by Google via one of its arms (i.e., YouTube) meant more power overall, not only in relation to YouTube, but also in the various other applications Google owns and controls and the markets they spin.[282] Additionally, and in a circular fashion, increased market power also meant increased collection of personal information.[283] Thus, failing to vigorously enforce privacy protections led to Google enjoying a free pass to enhance its dominance and squash competition.[284] The problem with this argument, however, is that it moves from critiquing Google for tramping over privacy in the process of achieving and deepening market power, to supporting the personal data market so long as it is competitive.[285]

4. Competition Regulators Follow the Wrong Cue from Privacy Regulators

One possible explanation for competition regulators' failure to fully grasp the value of privacy—or to avoid the familiar pitfalls of consent and control—is that privacy regulators themselves fall into these same traps, offering narrow and superficial interpretations of privacy. If this is the case, then by the time competition regulators address privacy in markets, the scales

279. FTC, STATEMENT OF JOSEPH J. SIMONS & CHRISTINE S. WILSON *REGARDING FTC AND PEOPLE OF THE STATE OF NEW YORK V. GOOGLE LLC AND YOUTUBE, LLC* 1 (2019), https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf [https://perma.cc/8H6C-63ZX].

280. CHOPRA GOOGLE DISSENT, *supra* note 278, at 1.

281. *See id.* at 2–3 ("Behavioral advertising, unlike contextual advertising, is about targeting each individual – a demographic of one. Google is able to do this by tracking and collecting an enormous amount of information on users' behavior wherever Google embeds its technology. This includes activity on their phones, home devices, on YouTube, and nearly everything they do online. . . . Google then monetizes these insights by using them to psychologically profile each user and predict in real time what content will be most engaging and which ads will be most persuasive. For any person, this is worrisome. But when it happens to a child, it can be illegal.").

282. *Id.* at 4 ("As a subsidiary of Google, YouTube is not an independent company. Google uses insights from other properties to enhance its targeting and monetization of YouTube, and it uses YouTube viewing behavior to better monetize its other properties. . . . By illegally collecting children's data on YouTube, Google can better monetize data collected from parents and children across properties, giving the company a clear competitive advantage when targeting them.").

283. *See id.* at 5–6.

284. *See id.*

285. *See id.*

are already tipped and the outcome predetermined by the way privacy regulators have framed the issue.

The FTC serves both as the United States' de facto privacy regulator[286] and as one of the country's main regulators tasked with enforcing competition and consumer protection more broadly.[287] Wearing its two hats, the FTC has generally expressed the view that privacy protections are either about privacy notice and choice (disclosure and consent), consumer choice generally, or data security.[288] That has been true for at least a decade,[289] and it is still true today; the focus on privacy disclosures, privacy consent, and consumer choice still dominates the FTC's approach. Significant enforcement actions brought by its Bureau of Consumer Protection (the privacy regulator hat) in 2024 were each grounded in respondents' use of data without consent.[290] In its most wide-ranging case against two data brokers, for example, the complaint from December 2024 "alleges that Gravy Analytics and Venntel violated the FTC Act by . . . collecting and using consumers' location data without obtaining verifiable user consent . . . . [and] continued to use consumers' location data after learning that consumers didn't provide informed consent."[291] The

286. *See, e.g.*, FTC Rich Comment 2014, *supra* note 267, at 1 (noting that the FTC is "the nation's leading consumer privacy enforcement agency"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

287. *See Bureau of Competition*, FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-competition [https://perma.cc/F745-VMD9] ("The FTC's Bureau of Competition enforces the nation's antitrust laws, which form the foundation of our free market economy.").

288. *See, e.g.*, FTC Rich Comment 2014, *supra* note 267, at 3; FTC 2016 REPORT, *supra* note 270, at i; FTC, STATEMENT OF COMMISSIONER ROHIT CHOPRA JOINED BY COMMISSIONER REBECCA KELLY SLAUGHTER *REGARDING DATA SECURITY AND THE SAFEGUARDS RULE* 1 (2020), https://www.ftc.gov/system/files/documents/public_statements/1567795/final_statement_of_rchopra_re_safeguards.pdf [https://perma.cc/J5YC-E6NL] (expressing concerns about data security).

289. *See, e.g.*, Letter from Jessica L. Rich, *supra* note 42, at 3; Solove & Hartzog, *supra* note 286, at 628; BAMBERGER & MULLIGAN, *supra* note 195, at 68–69 (describing the development of the FTC's emergence as a privacy regulator).

290. *See* Press Release, FTC, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data [https://perma.cc/KQ54-AD3M] ("Data aggregator InMarket Media will be prohibited from selling or licensing any precise location data to settle Federal Trade Commission charges that the company did not fully inform consumers and obtain their consent before collecting and using their location data for advertising and marketing."); Press Release, FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data [https://perma.cc/4RNS-TPGD] ("FTC charges X-Mode and Outlogic with selling raw location data, failing to obtain informed consumer consent."); Press Release, FTC, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers [https://perma.cc/FM39-W92S].

291. Press Release, FTC, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, *supra* note 290.

enforcement focus on consent exists not only in the relatively easy case of data brokers, which will typically not have consumer consent as an indirect third party,[292] but with firms that have a direct relationship with consumers as well.[293]

Even in an elaborated and important staff report from September 2024, where the FTC timely points to the many problems with the current data economy and its harmful ways,[294] the FTC largely equates privacy harms with lack of consent and lack of control by consumers.[295] The report does not challenge the foundations of surveillance capitalism; it merely proposes tempering its excesses by invoking data minimization and consumer-friendly privacy policies while articulating yet another "putting consumers in control" agenda—the very approach that contributed to the current problems.[296]

In April 2024, the FTC's Bureau of Consumer Protection outlined its approach to privacy enforcement.[297] Although the agency has offered a well-founded critique of the "notice-and-choice regime"—closely aligned with what we call consent, control, and choice[298]—some of the key examples presented as evidence of the FTC's efforts to shift away from this failed regime continue to rely on notice-and-consent-based enforcement. Although the FTC has also pointed to other regulatory strategies,[299] its ongoing reliance on consent-based mechanisms underscores the difficulty of fully breaking away from this ineffective framework, with significant consequences for privacy protection.

---

292. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 146–47 (2016).

293. *See* Press Release, FTC, FTC Says Genetic Testing Company 1Health Failed to Protect Privacy and Security of DNA Data and Unfairly Changed Its Privacy Policy (June 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-1health-failed-protect-privacy-security-dna-data-unfairly-changed [https://perma.cc/PL3U-S2NG] ("The Federal Trade Commission charged that the genetic testing firm 1Health.io left sensitive genetic and health data unsecured, deceived consumers about their ability to get their data deleted, and changed its privacy policy retroactively without adequately notifying and obtaining consent from consumers whose data the company had already collected.").

294. *See generally* FTC SOCIAL MEDIA REPORT, *supra* note 24.

295. *See, e.g.*, *id.* at v–vi.

296. *See id.* at vii.

297. *See generally* Samuel Levine, Bureau Consumer Prot., Remarks at the Fourth Annual Reidenberg Lecture at Fordham Law School: Toward a Safer, Freer, and Fairer Digital Economy (Apr. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf [https://perma.cc/3E5H-285W]; Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen, *After Notice and Choice: Reinvigorating "Unfairness" to Rein in Data Abuses*, 77 STAN. L. REV. 1375 (2025).

298. Khan et al., *supra* note 297, at 1378–81.

299. *See, e.g.*, Levine, *supra* note 297, at 10–11 (mentioning data minimization); *id.* at 13 ("[W]e have been using our rulemaking authority to establish across-the-board protections, including by proposing a market-wide ban on hidden fees, a requirement to make subscriptions easy to cancel, and limits on nudges that keep kids hooked."); *see also* Khan et al., *supra* note 297, at 1406–43 (identifying the pillars of the FTC's new consumer protection framework in the digital age).

In summary, regulators' first error lies in underestimating the importance of the right to privacy or misinterpreting its scope. They frequently reduce privacy to a superficial and technical concept, limited to issues like consent, control, or consumer choice. Moreover, they often regard privacy as merely an intermediate value—a tool to support broader economic protections—rather than recognizing it as a fundamental right in its own right. Specifically, this approach that views privacy as a tool to advance other goals ultimately comes at the expense of privacy itself. Taking the wrong cue from privacy regulators, competition law fails to define privacy in a way that engages with privacy's economic implications[300] or encompasses real protection from surveillance. Moreover, by prioritizing other economic objectives, regulators not only fail to eliminate the surveillance enterprise but actively justify it, ultimately providing a framework within which surveillance firms are legitimized even though they are destructive to privacy. By contrast, a truly privacy-focused approach would address surveillance at its root.

B. THE SECOND ERROR: MISTAKING MARKETS

In the second type of error, competition regulators prioritize markets for surveillance[301] over markets for privacy. They do this by either being agnostic to the substance of the market and choosing to promote the more lucrative and thriving market for surveillance; by not fully internalizing that surveillance is exactly contradictory and devastating to privacy; or by suffering from conceptual confusion as to the difference between surveillance and privacy markets. This confusion is perhaps predictable, as the same firms—Google and Meta, for example—operate on both sides of a multisided information economy[302]: They dominate the surveillance-driven targeted advertising market for businesses while ostensibly providing privacy-focused services in consumer markets for search and social media. Although this duality is largely illusory—their business models fundamentally rely on data extraction to sustain the targeted-ads market, preventing them from truly offering privacy to consumers—it might explain part of the regulatory confusion. Whatever the reasons are, this confusion ultimately legitimizes and fosters surveillance, effectively shutting the door on any realistic prospect for privacy to prevail. Also, it combines with the thin definition of privacy to predetermine the winner when competition and privacy are balanced.

300. *See supra* Section II.A.1.

301. *See supra* notes 10–13 and accompanying text.

302. *See, e.g.*, Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333, 344 (2021) ("Often, a platform creates two connected markets: one facing consumers from whom data is extracted and the other facing other businesses that purchase either the data or a good into which the value of acquired data is impounded (for example, advertising slots).").

1. Legitimizing Surveillance Markets

One manifestation of this error can be seen in the FTC's traditional approach. The FTC has expressed views that the market for surveillance is legitimate (as long as it is sufficiently competitive) and that it can even be beneficial to consumers. For example, in 2016, former FTC Commissioner Maureen K. Ohlhausen participated in an "Advertising and Privacy Law Summit" and made remarks on the FTC's approach to protecting privacy.[303] Commissioner Ohlhausen hailed the use of online targeted advertising crediting it with the very success of the internet, though admitting that the "use of consumer data can raise privacy concerns."[304] Commissioner Ohlhausen noted that "[p]rivacy is a complex regulatory issue, in part because misguided privacy protections can preclude the massive benefits of data use and *increase* the harms from data misuse," no less.[305] At the time, there was a Federal Communications Commission ("FCC") rulemaking proposal aiming to regulate the privacy practices of broadband internet access service providers ("ISPs"). One of the main points of contention in the FCC's privacy rulemaking proposal was that it potentially hindered competition while increasing certain privacy protections in a way the FTC considered undesirable.[306] Directly addressing the complex relationship between competition and privacy, Commissioner Ohlhausen noted that "the FCC's framework places ISPs under a different set of regulations than those governing edge providers such as Google or Netflix, even though companies throughout the internet ecosystem collect and use significant amounts of consumer data."[307] With the intention of being "explicit," Ohlhausen stated that "these proposed rules would hamper ISPs from competing with other businesses to serve consumers in data-driven industries, including online advertising."[308] Instead of embracing or even encouraging the proposed limits on who may collect personal information and participate in the privacy-eroding targeted advertising industry, the FTC opposed restricting firms' ability to collect and commercially exploit personal data.

Another example is an FTC action from 2021 against an application provider, SpyFone, and its CEO.[309] The FTC found that they "sold stalkerware

303. *See* Maureen K. Ohlhausen, Comm'r, FTC, Reactions to the FCC's Proposed Privacy Regulations 1 (June 8, 2016), https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf [https://perma.cc/GHE4-NA7T].

304. *Id.*

305. *Id.* (emphasis added).

306. *Id.* at 6.

307. *Id.*

308. *Id.*

309. Press Release, FTC, FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data [https://perma.cc/KAK3-X33Y].

apps that allowed purchasers to surreptitiously monitor photos, text messages, web histories, GPS locations, and other personal information on the phone on which the app was installed without the device owner's knowledge,"[310] all done as well without proper security.[311] What was the remedy? An order banning a stalkerware provider and its CEO "from *the surveillance business*."[312] This choice of words is surprising but telling: There *is* a surveillance business and it is legitimate, and only those who do not play by the rules might be banned from it. An earlier case with similar facts did not raise a ban on the accused firm's activity.[313]

The FTC did not precisely define what is included in the "surveillance business." Based on the context, the FTC likely intended to highlight that stalkerware apps are undeniably part of the surveillance industry. But what about companies like Meta,[314] Google,[315] or even Apple[316] who are all known privacy offenders, even recidivists, and the broader multibillion-dollar targeted-advertising and surveillance capitalism sector?[317] The key point the FTC is making here, quite explicitly, is that the mere act of using surveillance as a business model is not inherently unlawful.

---

310. *Id.*

311. *Id.*

312. *Id.* (emphasis added).

313. *See* Press Release, FTC, FTC Brings First Case Against Developers of "Stalking" Apps (Oct. 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps [https://perma.cc/Z2EX-R4FP]. For a critique on the FTC's approach in the Retina-X case, see generally FTC, STATEMENT OF COMMISSIONER ROHIT CHOPRA *IN THE MATTER OF SPYFONE* (2021), https://www.ftc.gov/system/files/documents/public_statements/1595161/updated_date_final_chopra_statement_on_spyfone_.pdf [https://perma.cc/6QT3-NCGJ].

314. *See, e.g.*, FTC, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA *IN RE FACEBOOK, INC.* 2–4 (2019) [hereinafter CHOPRA FACEBOOK DISSENT], https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [https://perma.cc/44Z7-FRWD].

315. *See, e.g.*, CHOPRA GOOGLE DISSENT, *supra* note 278.

316. *See, e.g.*, The Associated Press, *Apple to Pay $95 Million to Settle Lawsuit Accusing Siri of Eavesdropping*, NPR (Jan. 3, 2025, 2:00 AM), https://www.npr.org/2025/01/03/g-s1-40940/apple-settle-lawsuit-siri-privacy [https://perma.cc/7VHV-6LX7] ("Apple has agreed to pay $95 million to settle a lawsuit accusing the privacy-minded company of deploying its virtual assistant Siri to eavesdrop on people . . . . The proposed settlement . . . resolve[d] a 5-year-old lawsuit revolving around allegations that Apple surreptitiously activated Siri to record conversations through iPhones and other devices equipped with the virtual assistant for more than a decade. The alleged recordings occurred even when people didn't seek to activate the virtual assistant . . . . Some of the recorded conversations were then shared with advertisers in an attempt to sell their products to consumers more likely to be interested in the goods and services, the lawsuit asserted.").

317. *See generally* Calvano & Polo, *supra* note 113.

2. Confusing and Conflating Markets for Privacy with Markets for Surveillance

In the second type of market-analysis error, regulators routinely confuse and conflate a market for privacy with a market for surveillance. They may begin their analysis by emphasizing the importance of privacy to consumers, treating it as a final good or a key quality of other goods. However, they then shift their focus to other concerns which turn out to be more consequential—the lack of competition in markets for surveillance, such as those for targeted advertising. In other cases, they consider a merger's impact on both consumers' privacy and competitors' ability to compete, but end up marginalizing privacy concerns and focusing on competitive levels in surveillance markets post-merger. This special focus reveals a deeper commitment to capitalism as a superior value rather than a genuine concern for privacy and other consumer and individual rights. And while sometimes regulators have expressed criticism about the lack of competition over privacy as a final good or as a quality of other goods, they also treat markets for surveillance as prima facie legitimate as long as they are considered to be sufficiently competitive.

This type of error appeared in merger review decisions that have highlighted the privacy-as-quality perspective to supposedly increase the importance of privacy in merger reviews. As discussed above,[318] in the 2014 Facebook–WhatsApp merger, the European Commission initially found that in the case of consumer communication applications, such as Facebook's Messenger and WhatsApp, firms compete over two primary parameters: the application functionalities and the size of the network.[319] The European Commission highlighted that the importance of "privacy and security" as application functionalities "varies from user to user but [they] are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues."[320] It also stressed that WhatsApp and Facebook have "no current plans to introduce advertising on WhatsApp post-Transaction,"[321] as an important feature of the merger and an indication that privacy and security are important to and valued by consumers. The European Commission also pointed to the positive relationship between privacy and security and market success, noting that "[t]he functionalities offered are at the heart of the consumer communications apps' value proposition to customers . . . in order to gain the largest user base."[322]

Surprisingly though, when the European Commission considered the possibility that the merger might harm privacy by degrading the application's quality and functionality, it reached a perplexing conclusion. Although

318. *See generally* FACEBOOK/WHATSAPP EC MERGER REVIEW, *supra* note 39.
319. *Id.* ¶ 86.
320. *Id.* ¶ 87.
321. *Id.* ¶¶ 168–70.
322. *Id.* ¶ 87.

Facebook has an incentive not to introduce targeted ads on WhatsApp to avoid user abandonment,[323] the European Commission found that even if it did, there would be sufficient competition *in the targeted advertising market* to prevent foreseeable harm to competition—but competition over what? The targeted advertising market is a market that is not even consumer-facing, not to mention focused on privacy, exactly the contrary.[324] This logical leap implies that the European Commission began its analysis by treating privacy as an important quality feature, but concluded by considering it irrelevant to the sort of competition it was concerned about. The primary focus on the business-facing targeted advertising market, rather than on a consumer-facing market for quality features such as privacy, was a recurring theme in the European Commission's review,[325] even though this approach contrasts with the European Commission's initial assertion that the proposed merger pertains to a "market for *consumer* communications services."[326]

A similar leap in analysis, from discussing potential issues with quality in consumer-facing markets to finding that competition levels are sufficient in business-facing surveillance markets, appeared in the European Commission merger review of the 2010 Microsoft–Yahoo merger, where Microsoft took over the Yahoo search business.[327] As noted above, the European Commission's review concluded that for "free" products and services like online search, the absence of price competition shifts the competitive focus primarily to the quality of the offering.[328] Discussions about the quality of free goods must take place in the context of the consumer side of the search market, where the goods are "free."[329] On the other side of the market, where ads and ad spaces are bought and sold, transactions obviously involve a price. Thus, it might seem that the regulatory concern was the foreseeable exploitation of consumer data against consumers in privacy-degrading ways resulting from the proposed merger. However, in the Microsoft–Yahoo case, the discussion of quality was somehow reframed in a way that worked against privacy, shifting the focus to the quality of the targeted ads shown to users—ads that are generated through surveillance—and to the scale and quality of user information fed into

323. *Id.* ¶¶ 173–74.

324. *Id.* ¶¶ 176–79.

325. *See also id.* ¶¶ 184–90.

326. *Id.* ¶ 20; *see also id.* ¶¶ 21–34.

327. *See generally* MICROSOFT/YAHOO! SEARCH BUSINESS EC MERGER REVIEW, *supra* note 114.

328. *Id.* ¶ 101.

329. *See supra* Section II.B; *see also* STIGLER COMMITTEE ON DIGITAL PLATFORMS, FINAL REPORT 30 (2019), https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms-committee-report-stigler-center.pdf [https://perma.cc/F7MM-3PFQ] ("Digital platforms are characterized by free services. 'Free' is not a special zone where economics or antitrust do not apply. Rather, a free good is one where the seller has chosen to set a monetary price of zero and may set other, non-monetary, conditions or duties. . . . [B]arter is a common way in which consumers pay for digital services. They barter their privacy and information . . . in exchange for digital services. However, in principle, that information has a market price that can be analyzed.").

targeted-ad platforms.[330] The European Commission found that "increased scale" and a "higher degree of user engagement" with "[h]igher [user] query volume" that "in turn, improve[] ad relevance and the likelihood that a user will click on an ad and ultimately convert his click into a purchase"—or, in other words, higher volume and increased quality of user information that was collected—would lead to a higher return on investment for firms.[331] Ultimately, the European Commission was not primarily concerned with the quality that consumers receive on their end but instead focused on the potential efficiencies that the merger might create in the surveillance market.

The U.S. DOJ apparently held the same view, finding that "[t]he search and paid search advertising industry is characterized by an unusual relationship between scale and competitive performance," and thus Microsoft's new access to a greater volume of query datasets would improve its ability to serve relevant search results and ads to users.[332] Consequently, the DOJ concluded that the Microsoft–Yahoo merger will allow the two firms to take on Google and intensify competition in the targeted marketing and search markets,[333] ignoring the privacy implications.

C. COMBINING ERRORS: THE FAILURE OF COMPETITION FOR PRIVACY

Together, regulatory errors in defining both privacy and markets render competition, as currently applied, an anti-privacy framework.

On the one hand, reductive views of privacy fail to account for the complexities of privacy in market dynamics and, more critically, overlook its inherent conflict with the dominant monetization strategies of firms in the digital economy. On the other hand, competition regulators' agnostic stance toward the nature of the markets they regulate leads to the same commitment to the promotion of surveillance markets, as any other market, regardless of the fundamental harms they impose. This oversight is further compounded by the analytical confusion that pervades market assessments in antitrust cases, whereby competition in the market for surveillance replaces competition in a theoretical market for privacy as the unit of analysis, even when the underlying question involves market constraints on privacy behaviors.

Together, these errors combine in a number of ways to reinforce the dominance of surveillance-driven business models at the expense of consumer

330. MICROSOFT/YAHOO! SEARCH BUSINESS EC MERGER REVIEW, *supra* note 114, ¶¶ 40, 101, 163; *see also* Mark A. Lemley, *The Contradictions of Platform Regulation*, 1 J. FREE SPEECH L. 303, 311–16 (2021) (discussing the confusion around defining a market in antitrust analysis of big tech firms).

331. *Id.* ¶ 163; *see* Esayas, *supra* note 109, at 154.

332. Press Release, U.S. Dep't of Just., Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc. (Feb. 18, 2010), https://www.justice.gov/opa/pr/statement-department-justice-antitrust-division-its-decision-close-its-investigation-internet [https://perma.cc/T59M-7RXS].

333. *Id.*

and civil rights. Most basically, where privacy and competition conflict, the calculus between a thin understanding of privacy and a robust commitment to market competition will consistently net a privacy loss—for even when privacy is reflected in the analysis, it is defined in a manner that does not meaningfully challenge the behavioral surveillance paradigm.

On a deeper level, even when privacy might align with competition, privacy will only be protected in service of promoting privacy-destructive markets. This paradox is exemplified in the German Facebook case, discussed above, which commentators have recognized as perhaps the most promising instance of using competition law to protect privacy because it recognized that privacy violations might form the bases for a competition claim.[334] In its decision, the German competition regulator prohibited Facebook from combining user data from its various services and third-party sources without user consent.[335] The rationale was that such data combination granted Facebook an unfair advantage in surveillance markets.[336] Although this action ostensibly aligns with privacy considerations[337]—similar to the Google–Fitbit case, where reducing data concentration could mitigate surveillance, a regulatory rarity—the German case exposes the two critical regulatory errors we analyze that undermine privacy protections, even when privacy and competition concerns supposedly align.

First, the firm conduct in question, deemed anticompetitive, is required to violate a limited and overly narrow definition of privacy—consent, control, and choice. Second, the privacy-destructive conduct must also be shown to harm competition within the surveillance market. Ironically, then, privacy is credited in competition analysis when it helps to promote the health and competitiveness of privacy-eroding surveillance markets.

III. IF YOU WANT TO REGULATE, REGULATE

Competition law, as a body of regulation that surfaces and seeks to address abuses arising from market power and size, holds, to be sure, an intuitive allure for those concerned with dominant firms' practices that persistently degrade privacy. Yet untangling the relationship between competition and privacy concerns—along with regulators' errors that always ensure a doctrinal thumb on the scale in favor of competition—reveals that competition law is not only an inappropriate but even a dangerous vehicle for driving privacy protection.

As this Article has explored, competition's focus on concentration of data as a business asset might in individual cases embrace privacy-protective

334. *See also supra* notes 44–47 and accompanying text.

335. Press Release, Bundeskartellamt, *supra* note 44.

336. *See, e.g.*, Kerber & Zolna, *supra* note 45, at 219; Graef et al., *supra* note 45, at 210 (noting the Bundeskartellamt's approach and advocating for "[d]ata protection and consumer law principles as benchmarks for exploitative abuse").

337. *See* Kerber & Zolna, *supra* note 45, at 222.

remedies, but it will not systematically. And it will do so, as the German Bundeskartellamt's case against Facebook discussed above demonstrates, in the zero-sum context in which regulators conclude that those remedies will *serve the health of privacy-destructive surveillance markets*. Moreover, even when treated as a component of product or service quality, privacy will lose out given competition law's legitimization and promotion of those markets. Because the notion of a market for privacy is an illusory one,[338] firms can continue, without competitive constraint, to degrade privacy practices. Thus, even in the limited scenarios in which competition and privacy concerns might align, any hopes at reliably protecting privacy against the behavior of market giant platforms through the back door of competition should be checked at that door's threshold.

These insights, we argue, further fuel the need to go through the front door and to use competition law's insights about concentration and power to regulate data practices and markets directly, in service of privacy. The lens of competition, and the identification of the contexts in which competition concerns align with those of privacy, point to the ways in which large data-extractive firms and the markets in which they operate might be treated through direct privacy regulation. As a regulatory matter, it is competition law's interventions mandating substantive behavioral limits on the collection, combination, and use of data owned by businesses along a metric of data minimization where privacy alignment is achieved. And as an analytic matter, a competition and privacy alignment is achieved by the recognition that the absence of market constraints on surveillance behavior—constraints that will not arise spontaneously—allows dominant firms to degrade privacy. Lock-in renders this degradation durable.

Some regulators have taken tentative steps in the direction of regulating surveillance behavior directly, in the absence of market constraints. Former FTC Commissioner Chopra offered a critical voice to the Commission's decisions that reflect the two analytic errors we describe here, notably dissenting[339] from the Commission's resolution of its investigation of Facebook after the Cambridge Analytica scandal, on payment by Facebook of a $5 billion penalty.[340] In Commissioner Chopra's statement in that matter, he

338. *See* Pasquale, *supra* note 3, at 1022 ("It is hard to imagine an online world in which users care deeply about purchasing privacy, or even consider it carefully as a quality of the service they are using. This is not because the users don't care about privacy. Rather, consumers have little to no real choice in the matter because the dominant services are so superior to also-ran competitors. Dominant firms see little to no reason to compete to improve their privacy practices when users are so unlikely to defect. A lemons equilibrium prevails."); *see also* Lemley, *supra* note 330, at 328 ("We need to choose one benefit at the expense of the other, or balance the two, accepting, for instance, less privacy in order to have more competition or vice versa.").

339. *See generally* CHOPRA FACEBOOK DISSENT, *supra* note 314.

340. Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases

recognized that the real problem was not simply specific deceptive practices, but the company's "behavioral advertising business model" itself, which "is both the company's profit engine and arguably the root cause of its widespread and systemic problems."[341] "[B]ehavioral advertising," he wrote, "allows advertisers to use mass surveillance as a means to their undisclosed and potentially nefarious ends . . . . [y]et Facebook's advertising model allows almost anyone to pay for access to this powerful tool."[342] In that light, he argued that the FTC order "places no meaningful restrictions on Facebook's ability to collect, share, and use personal information," and "does not require . . . actually respecting user privacy."[343] Thus, he concluded that he does "not believe a $5 billion penalty, *especially as part of a settlement that otherwise blesses the company's business model*, will restore the public's confidence or vindicate [the FTC's] authority."[344]

These remarks reflect an understanding of the two critical regulatory errors we identify. In the months before February 2025, when former Commissioner Chopra was removed from his subsequent post as director of the Consumer Financial Protection Bureau by President Donald Trump,[345] the agency had begun moves to use its authority to intervene in questions of surveillance markets, issuing guidance limiting employer use of third-party data dossiers about their workers,[346] and requesting public comment "on strengthening privacy protections and preventing harmful surveillance in digital payments, particularly those offered through large technology platforms."[347]

In 2022, the FTC under the lead of Chair Lina Khan pointed even more encouragingly in this direction, launching a rulemaking and inviting "public comment on the harms stemming from commercial surveillance and whether new rules are needed to protect people's privacy and information."[348] Although

/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/Q4XS-525N].

341. CHOPRA FACEBOOK DISSENT, *supra* note 314, at 2.

342. *Id.* at 3.

343. *Id.* at 12.

344. *Id.* at 17 (emphasis added).

345. *See* Editorial Board, *Rohit Chopra Is Ousted, at Last*, WALL ST. J. (Feb. 2, 2025, 5:31PM), https://www.wsj.com/opinion/rohit-chopra-is-ousted-at-last-trump-fires-warren-protege-and-cfpb-could-now-be-shut-down-ed6958f2? (on file with the *Iowa Law Review*) (lauding the ouster).

346. *See CFPB Takes Action to Curb Unchecked Worker Surveillance*, CONSUMER FIN. PROT. BUREAU (Oct. 24, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-curb-unchecked-worker-surveillance [https://perma.cc/SVB3-6PW7] (describing agency guidance making such data markets subject to the requirements of the Fair Credit Reporting Act).

347. *CFPB Seeks Input on Digital Payment Privacy and Consumer Protections*, CONSUMER FIN. PROT. BUREAU (Jan. 10, 2025), https://www.consumerfinance.gov/about-us/newsroom/cfpb-seeks-input-on-digital-payment-privacy-and-consumer-protections [https://perma.cc/SY6K-4UQ4].

348. Press Release, FTC, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-r

critics debate whether the scope of the FTC's authority to prohibit unfair acts would extend to such a rulemaking and the ultimate form of such a rule has not been released, Commission staff have expressed a commitment to moving toward a "proactive approach to privacy" that "represents the tip of the spear in a broader rethinking of the government's role in making markets work better."[349] The rulemaking has, moreover, provided the opportunity for leading privacy groups to weigh in on what market-wide regulations might consist of, including restrictions on collection, retention, use, and sharing of data to promote data minimization,[350] a general ban on targeting ads to individuals based on online behavior, and on the use by ad deliverers of user lists collected by data brokers through the tracking of user behavior.[351]

Although former FTC Chair Khan resigned on January 21, 2025, leaving the future of the commercial surveillance rulemaking in question, bipartisan members of Congress on a parallel track have been working in this direction. They introduced the Banning Surveillance Advertising Act, which would enable regulators—including the FTC and state attorneys general—and also private individuals to enforce a ban on the use of targeted ads based on personal data altogether.[352] By whoever's hand, ultimately, the problem of surveillance markets dominated by large firms will not be addressed without regulating the market for personal data directly, just as we do in other contexts plagued by market failures, where the underlying behaviors are harmful.[353]

---

eleases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/C7Y4-9CCF].

349. Levine, *supra* note 297, at 18.

350. *See* Elec. Frontier Found., Comment Letter on Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 2 (Nov. 21, 2022) [hereinafter EFF FTC Comment], https://www.regulations.gov/comment/FTC-2022-0053-1014 [https://perma.cc/92C7-RXGW]; *see also* Elec. Priv. Info. Ctr., Comment Letter on Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 30–32, 66–67 (Nov. 21 2022), https://www.regulations.gov/comment/FTC-2022-0053-1195 [https://perma.cc/9XQ5-HKVP] (discussing minimization rules).

351. *See* EFF FTC Comment, *supra* note 350, at 7–8.

352. Vasundhara Majithia, *The Banning Surveillance Advertising Act: What the Clampdown on Targeted Advertising Means for the Internet Economy*, BERKELEY TECH. L.J. (Apr. 23, 2022), https://btlj.org/2022/04/the-banning-surveillance-advertising-act-what-the-clampdown-on-targeted-advertising-means-for-the-internet-economy [https://perma.cc/9L2N-QT6X].

353. *See* Robert Hackett, *Harvard Economist Calls for Outlaw of Online Advertising Markets—Just Like the Trade of 'Organs, Babies, or Slaves,'* FORTUNE (Nov. 18, 2019, 1:41PM), https://fortune.com/2019/11/18/google-facebook-online-advertising-ban-surveillance-capitalism [https://perma.cc/5QBY-9GUR] (arguing for a ban on ad markets).