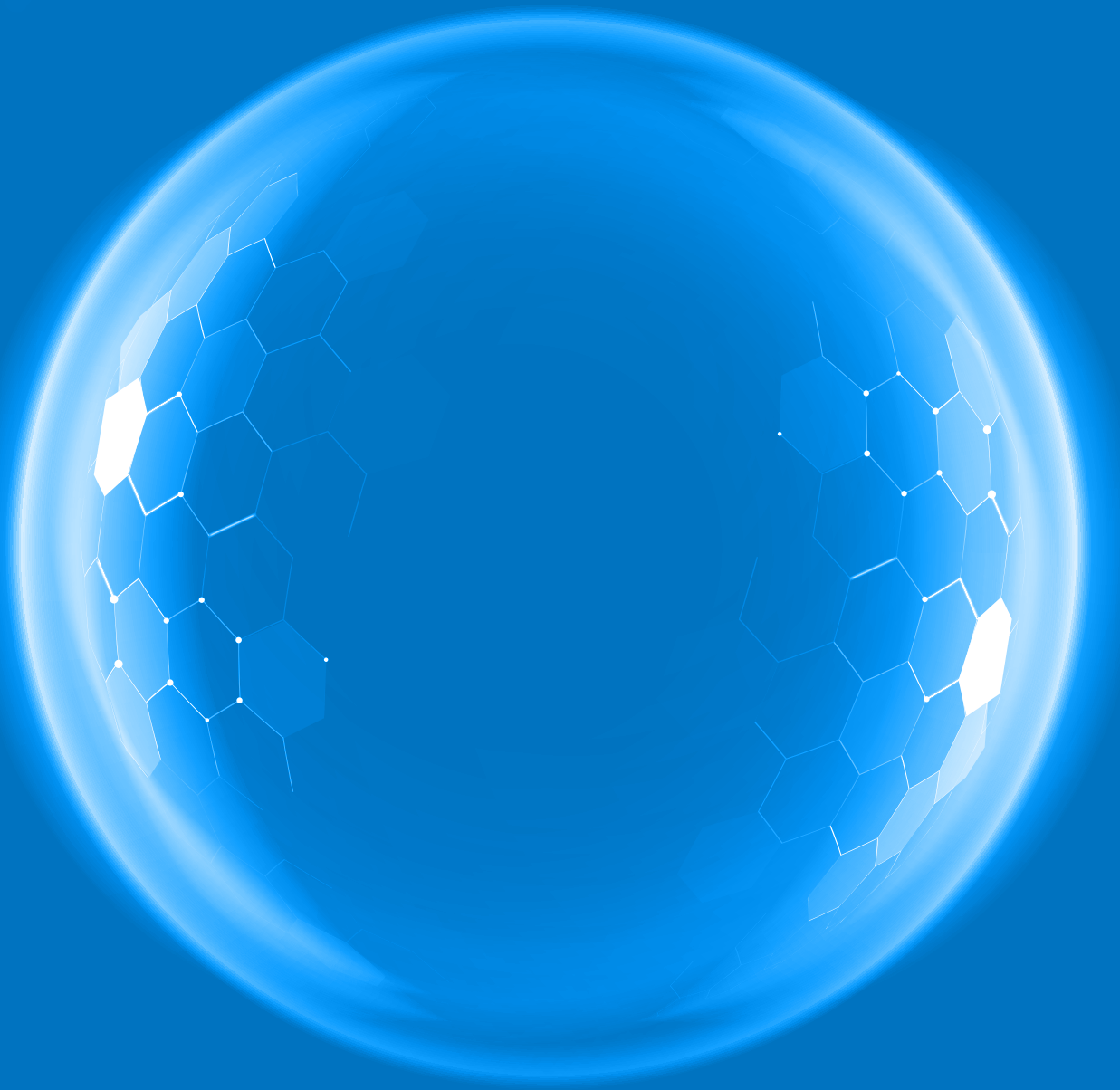
PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT



BY DANIEL A. HANLEY & KARINA MONTOYA[1]

1 Daniel A. Hanley is a Senior Legal Analyst at the Open Markets Institute. Karina Montoya is a Reporter-Researcher with the Center for Journalism & Liberty, a program of the Open Markets Institute.

CPI ANTITRUST CHRONICLE DECEMBER 2022

DIGITAL PLATFORMS IMPLEMENT PRIVACY-CENTRIC POLICIES: WHAT DOES IT MEAN FOR COMPETITION?
By Reinhold Kesler

HARMING COMPETITION AND CONSUMERS UNDER THE GUISE OF PROTECTING PRIVACY: REVIEW OF EMPIRICAL EVIDENCE
By D. Daniel Sokol & Feng Zhu

EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION
By Alex Marthews & Catherine Tucker

POPULAR MOBILE APPS IN THE PANDEMIC ERA: A GLIMPSE AT PRIVACY AND COMPETITION
By Ginger Zhe Jin, Ziqiao Liu & Liad Wagman

PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT
By Daniel A. Hanley & Karina Montoya

HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?
By Giuliana Galbiati & Henri Piffaut

TOWARDS DATA PORTABILITY AND INTEROPERABILITY UNDER BRAZILIAN COMPETITION LAW: CRAFTING APPROPRIATE LEGAL STANDARDS FOR ABUSE OF DOMINANCE
By Victor Oliveira Fernandes

Visit www.competitionpolicyinternational.com for access to these articles and more!

PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT

By Daniel A. Hanley & Karina Montoya

Daniel A. Hanley & Karina Montoya comment on how antitrust enforcement can operate as a vital supplement providing consumers with robust privacy protections, despite the lack of a comprehensive federal law. The authors argue that antitrust enforcement can be used to provide consumers baseline privacy protections by (1) creating a market for privacy protections, (2) targeting specific conduct such as mergers, monopolization, and deception, and (3) courts imposing broad structural remedies inhibiting and deterring future violative conduct.

I. INTRODUCTION

In recent years, powerful technology corporations Google and Meta (the parent company of Facebook) have successfully eluded meaningful regulation by U.S. lawmakers, raising the question of what legal approach would most effectively bring them to heel.[2] Lawmakers and advocates increasingly consider privacy law and antitrust enforcement as the most potent legal avenues capable of taming Big Tech. Both areas of law are now seen as vehicles for a fundamental restructuring of the technology industry, one that would promote competition, curtail unfair practices such as self-preferencing, break up monopoly power, and provide protections to consumer privacy.

Unlike in other countries,[3] the United States does not have a general law that protects consumer privacy rights. Instead, privacy regulations exist through a patchwork of narrowly targeted and discrete laws, most of which predate the internet, and are enforced by an alphabet soup of federal and state agencies.[4]

At the national level, the Federal Trade Commission ("FTC") is the *de facto* federal privacy regulator because the agency can regulate data usage, acquisition, and user privacy through Section 5 of its originating statute, which grants it expansive authority to prohibit unfair or deceptive acts or practices as well as unfair methods of competition throughout the entire economy.[5]

Without a comprehensive privacy and data law, the predominant protections afforded to consumers over how their data is collected and used is through corporation-provided notices, which ultimately force users to agree to lengthy, non-negotiable, and near incomprehensible terms of service contracts.[6]

In the absence of comprehensive federal protection, states started to exercise their legislative powers about five years ago and enacted their own laws to protect consumer privacy. The first enacted law was California's Consumer Privacy Act ("CCPA") in 2018.[7] CCPA established several rights for Californians that give them more control of their personal data, including the right to know what information is collected and shared about them, to opt out from the sale of such data for advertising purposes, and the right to have it deleted as well. In 2020, California strengthened the CCPA by adding more requirements and created the state's first privacy protection agency, incentivizing other states to enact similar laws that will go into effect next year.[8]

Action from Congress and federal agencies have also moved forward. The American Data Privacy and Protection Act,[9] a breakthrough bipartisan bill to establish federal data privacy protections, is ready for a full House vote. Among other actions, while Congress considers legislation, the FTC has initiated a rulemaking to crack down on commercial surveillance.[10]

These recent efforts to enact privacy regulations are both admirable and necessary, but without the passage of a federal law like the American Data Privacy and Protection Act, federal enforcers see antitrust law as an essential supplement to check the power of Big Tech and create the opportunity for consumers to be provided some much-needed privacy protections. Recent examples of this effort include the Depart-

2 See Cat Zakrzewski, *Tech Companies Spent Almost $70 Million Lobbying Washington in 2021 as Congress Sought to Rein in Their Power,* Wash. Post (Jan. 21, 2022), https://www.washingtonpost.com/technology/2022/01/21/tech-lobbying-in-washington/.

3 For example, the European Union enacted the General Data Protection Regulations in 2018. See Danny Palmer, *What is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZD Net (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

4 See generally Daniel J. Solove, *A Brief History of Information Privacy Law*, Gwu. L. Fac. Pub. & Other Works (2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications. For a list of the major sector specific laws governing privacy, see Stephen P. Mulligan & Chris D. Linebaugh, Cong. Research Serv., R45631, *Data Protection Law: An Overview*, 7-35 (2019).

5 15 U.S.C. § 45; Erika M. Douglas, *The New Antitrust/data Privacy Law Interface*, 130 Yale L.J. Forum 647, 651 (2021).

6 Frank Pasquale, *Privacy, Antitrust, and Power*, 20 Geo. Mason L. Rev. 1009, 1012 (2013); Maurice E. Stucke, "Should We Be Concerned About Data-Opolies?," 2 Geo. L. Tech. Rev. 275, 289 (2018); James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, U. Ill. J.L. Tech. & Pol'y, Spring 2005, at 1, 2 (describing the development and proliferation of privacy policies among internet services).

7 Cal. Civ. Code § 1798.140.

8 Id. § 1798.199.10 (establishing the California Privacy Protection Agency). For a list of other state privacy laws, see Sheila A. Millar & Tracy P. Marshall, *The State of U.S. State Privacy Laws: A Comparison*, Nat'l L. Rev. (May 24, 2022), https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison.

9 *H.R.8152 - American Data Privacy and Protection Act*, Congress.gov, https://www.congress.gov/bill/117th-congress/house-bill/8152 (last visited Nov. 15, 2022).

10 Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

ment of Justice's lawsuit against Google's prolific use of restrictive agreements to maintain its dominant position in internet search, and the FTC's lawsuit challenging Meta's acquisitions of WhatsApp and Instagram.[11]

Traditional scholars have voiced significant skepticism with using antitrust to facilitate privacy protections. Their skepticism stems from at least three sources. First, scholars assert that privacy is merely a narrow situationally dependent consumer preference.[12] Second, traditional antitrust scholars assert that, under the predominant analytical framework governing antitrust law over the last four decades, antitrust has a narrow focus, which is primarily to prevent price increases to consumers and collusive behavior and, thus, should not be used to facilitate privacy protections for consumers.[13] Third, advocates have generally been unsuccessful with providing an articulable and comprehensive framework for how antitrust policy can both protect and facilitate data privacy while also facilitating robust and fair competition between firms.[14]

This Article attempts to ease the tension between antitrust law and privacy by detailing their complementary nature – the need for which has become more apparent since July 2021 when President Biden issued a sweeping executive order calling for increased market competition, in part, by prioritizing the protection and enhancement of data privacy rights and antitrust enforcement.[15]

II. DATA ACQUISITION AND PRIVACY ARE FUNDAMENTAL ASPECTS OF COMPETITION IN TECHNOLOGY MARKETS

Data and privacy are often at odds with one another: more of one typically means less of the other. Technology companies typically collect data as a byproduct of user action (e.g. a user's browsing history), but it can also be purchased from exchanges and collected from other tools that track users across the internet.[16] Privacy defines the limits on and the rules governing data collection by corporations. In many cases, due to the diverse ways services and applications are collecting and using data, privacy cannot achieve a singular goal or even be considered categorically good. For example, if a search engine was completely barred from collecting at least some, even anonymized, data from its users, it might be exceptionally difficult to increase the relevancy of search results and provide a quality product to consumers that can compete effectively.[17] In some cases, fewer privacy protections are warranted; in others, more is warranted.[18] However, when privacy is described as merely governing data collection, and when data is reduced to a benign byproduct of users' actions, this incomplete picture misses the critical nature of this key resource being bartered in technology markets.

Simply stated, data and privacy rules governing how data is collected, used, and sold are a fundamental aspect of the technology industry's competitive environment. Indeed, data is the foundational element atop which technology companies build their business operations; it is the market they operate in.[19] Without the ability to acquire as much data as possible from consumers with impunity, it is doubtful that modern internet titans such as Google and Meta would exist in their current forms. Given that many of the services provided by technology companies are free, privacy protections afforded to consumers are an essential non-price variable of product quality.

11 Amended Complaint, *United States v. Google LLC*, No. 20-03010 (D.D.C. Jan. 15, 2021); First Amended Complaint for Injunctive and Other Equitable Relief, *Fed. Trade Comm'n v. Facebook, Inc.*, No. 20-03590 (D.D.C. Aug. 19, 2021) (hereinafter "FTC Facebook Complaint").

12 See generally Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 Antitrust L.J. 121, 151-52 (2015).

13 See, e.g. Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, Antitrust Source, Dec. 2014, at 1 ("the acquisition and use of big data by online firms is not the type of conduct captured by the antitrust laws."), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf; see Lina Khan & Sandeep Vaheesan, *Market Power and Inequality: The Antitrust Counterrevolution and Its Discontents*, 11 Harv. L. & Pol'y Rev. 235, 270-71 (2017) (describing the goals and beliefs of the Chicago School of Economics that Robert Bork advocated for).

14 Allen P. Grunes, *Another Look at Privacy*, 20 Geo. Mason L. Rev. 1107, 1127 (2013); Douglas, *supra* note 5, at 658, 667.

15 Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 14, 2021).

16 Daniel A. Hanley, *A Topology of Multisided Digital Platforms*, 19 Conn. Pub. Int. L.J. 271, 294, 303-05, 319 (2020).

17 See generally Maurice E. Stucke & Allen Grunes, *Big Data and Competition Policy*, 289 (2016) (explaining the need for data-based businesses to obtain minimum efficient scale to be viable competitors).

18 Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1090 (2002); Pasquale, *supra* note 6, at 1016-17.

19 See Stucke & Grunes, *supra* note 17, at 277; see also Pasquale, *supra* note 6, at 1009.

For firms, data (and access to it) bestows several significant and, in some cases, insurmountable competitive advantages over rivals.[20] Here we list two of the primary advantages. First, data has exceptional scaling effects. The more data that can be collected, the more inferences can be made about the subject matter providing the data.[21] The ability to make inferences based on the data collected dramatically enhances the ability of the data collector to offer a sellable product to customers, which, too, can be a significant driver in both acquiring and retaining users.[22]

For example, targeted advertising products are based on tech giants following users across the web — for the most part unbeknownst to them — to build near-comprehensive profiles advertisers use to reach them across various digital publications, whether they be the websites of *The New York Times*, and *The Wall Street Journal,* or mobile apps.[23] The inferences Google makes about users' behavior, based on their browsing history or navigational maps usage for example, are also incorporated into these profiles, something that other publishers cannot do and offer to advertisers.

Indeed, the scaling effects can be so significant that a market often moves toward consolidating to only one or several participants, increasing barriers to market entry as well.[24] In that case, potential firms would have to provide similar or superior service in order to have a successfully competing product — which is inexorably tied to data acquisition and the number of pre-existing users.[25]

Second, when data is the operating principle behind the development and marketing of products within the technology industry, access to it determines whether that product or service exists at all. For example, one of the reasons no meaningful competitor has been able to challenge Google's dominance in internet search is because, given bandwidth and website ownership limitations, only so many competing search engines can scan a website at a time to feed into search results.[26]

When combined, these factors incentivize technology giants to collect as much data as possible, integrate psychologically manipulative tactics and technical hurdles into products that make it difficult for consumers to switch providers, and degrade privacy protections so that more data can be extracted.[27] Firms that share their data can even act as gatekeepers and selectively choose who has access to their data or not, creating a sub-market that becomes heavily reliant on access to that data.[28] Such a situation creates an opportunity for market foreclosure, where a company is not able to compete effectively because its access to the data was closed off.[29] For example, when Vine, a precursor to the video-sharing platform TikTok, started to present itself as a competitor to Meta, Mark Zuckerberg personally shut off Vine's access to specific Facebook data channels.[30]

As a legal regime based on limiting access to data and defining the methods of how it is acquired, used, and sold, the market rules governing privacy, therefore, are a fundamental component of how technology markets are structured.

---

20 Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 Ariz. L. Rev. 339, 346-47 (2017).

21 Stucke, *supra* note 6, at 283.

22 *Id.* at 321; Eliana Garcés & Daniel Fanaras, *Antitrust, Privacy, and Digital Platforms' Use of Big Data: A Brief Overview*, 28 Competition: J. Anti., UCL & Privacy Sec. Cal. L. Assoc. 23, 24 (2018).

23 Hanley, *supra* note 16, at 311.

24 *Id.* at 282, 289-90; Pasquale, *supra* note 6, 1015-16; Salil K. Mehra, *Data Privacy and Antitrust in Comparative Perspective*, 53 Cornell Int'l L.J. 133, 140-41 (2020).

25 Hanley, *supra* note 16, at 289-91.

26 Daniel A. Hanley, *Let's Make Google Share Some Secrets*, Wash. Monthly (July 20, 2021), https://washingtonmonthly.com/2021/07/20/lets-make-google-share-some-secrets/; Allen P. Grunes & Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, 14 Antitrust Source, Apr. 2015, at 8.

27 Maurice E. Stucke & Allen P. Grimes, *Debunking the Myths over Big Data and Antitrust*, Competition Pol'y Int'l: Antitrust Chronicle, May 2015, at 1, 9; Stucke, *supra* note 6, at 285-86.

28 Stucke, *supra* note 6, at 304-05.

29 Hanley, *supra* note 16, at 322.

30 See Adi Robertson, *Mark Zuckerberg Personally Approved Cutting Off Vine's Friend-Finding Feature*, Verge (Dec. 5, 2018), https://www.theverge.com/2018/12/5/18127202/mark-zuckerberg-facebook-vine-friends-api-block-parliament-documents.

III. ANTITRUST IS AN ESSENTIAL LEGAL TOOL FOR SECURING CONSUMER PRIVACY RIGHTS AND STRUCTURING BUSINESS CONDUCT TO PROTECT PRIVACY

U.S. antitrust law originated in the late 19th century out of the need to restrain unfair practices engaged in by dominant corporations in order to preserve the vitality of the democratic governance of markets and promote nationwide economic opportunity.[31] Recognizing its general economy-wide application, Congress purposefully designed the antitrust laws to be exceptionally broad. Antitrust governs all aspects of firm rivalry and creates a legal floor of acceptable business conduct. Almost no method of competition is outside the purview of the antitrust laws.[32]

Antitrust law can target "every" unreasonable restraint of trade or monopolization tactic, as well as exclusive deals, tying, and mergers that "may be substantially to lessen competition, or tend to create a monopoly."[33] Giving additional strength to the antitrust laws is the Supreme Court's interpretation that the antitrust laws have "dynamic potential" not confined to particular practices and were to be aimed broadly at all of the "economic consequences" of business conduct.[34]

The restrictions on businesses imposed by the antitrust laws accomplish two primary goals. First, by limiting a plethora of business conduct, antitrust law ensures businesses are competing fairly, implicitly incentivizing firms to avoid unfair methods of competition and, instead, engage in socially beneficial conduct that maximizes benefits to the public. Such socially beneficial conduct can include increasing investments into research and development, increasing product quality, and increasing pay to workers. Second, antitrust prevents and remedies undue concentrations or exercises of corporate power that entrench and expand a firm's dominant control. Antitrust enforcement can thus promote competition, increase consumer choice, and enhance product quality.[35]

Endowed with exceptional flexibility regarding restricting unfair business practices, antitrust enforcement can complement privacy goals and facilitate notable privacy protections in at least three ways to ensure that corporations are protecting user data, ensuring the highest quality product to consumers, and engaging in fair competition regarding the gathering, use, or access to user data.[36]

First, antitrust enforcement, in general, can facilitate privacy protections by creating a market for privacy protections. Against the backdrop of decades of anemic antitrust enforcement and profound increases in market concentration since the 1970s,[37] a "race to the bottom" has occurred in the technology industry that has caused privacy-centric products to be unable to compete effectively against their data-dependent competitors and has allowed services to extract as much data as possible.[38]

For example, when it comes to search, social media, e-commerce, digital advertising, and a host of other markets, all are dominated by a few companies — and no meaningful competitor has emerged in decades.[39] Given the dependency on data for the technology industry, the prospect of obtaining a monopoly position by acquiring as much data as possible, and its essential role in supporting the creation of many products and services, it is clear that "natural" market forces geared toward data extraction are unable to provide consumers with robust privacy protections.

---

31 See 21 Cong. Reg. 3151, 1352 (1890) (statement of Sen. Hoar) (Section 2 of the Sherman Act regulates the "means which prevent other men from engaging in fair competition with him[.]")

32 Obviously, there are notable exemptions from the antitrust laws. See, e.g. 15 U.S.C. § 17 (exempting labor union activity from the antitrust laws).

33 15 U.S.C. §§ 1, 2, 13, 18.

34 *Bus. Elecs. Corp. v. Sharp Elecs. Corp.*, 485 U.S. 717, 731-32 (1988).

35 Sandeep Vaheesan, *The Profound Nonsense of Consumer Welfare Antitrust*, 64 Antitrust Bull. 1, 2-3 (2019).

36 *Nat'l Soc. of Pro. Engineers v. United States*, 435 U.S. 679, 695 (1978) ("all elements of a bargain - quality, services, safety and durability[.]").

37 See Michael Kades, *The State of U.S. Federal Antitrust Enforcemen*t, Equitable Growth (Sept. 2019); Gustavo Grullon et al., *Are US Industries Becoming More Concentrated?* 23 Rev. Fin. 697 (2018).

38 Grunes, *supra* note 14, at 1112; Hanley, *supra* note 16, at 303-05.

39 Hanley, *supra* note 16, at 346-49.

By being able to increase competition in an industry and prohibiting a myriad of business practices that cause adverse effects on consumers and market competition,[40] antitrust law fundamentally shapes and incentivizes how businesses compete and the methods of competition they use to succeed in the marketplace.[41] In other words, antitrust law, like privacy protection, is essential to structuring a market — in this case, creating the market conditions necessary to make privacy a feasible goal for firms to provide to consumers, and inhibit firms from invading a user's privacy and use data in unfair ways that entrench or expand a firm's dominance.[42]

Second, antitrust enforcement can ensure privacy protections by targeting three types of violative conduct — mergers, monopolization tactics, and deception. Technology companies have long used mergers as an essential method of competition to acquire data and entrench their market position. Between 1987 and 2019, Google, Meta, Microsoft, Apple, and Amazon acquired 760 companies.[43] Evidence shows that mergers have been critical to degrading privacy protections. For example, before being acquired by Meta, the communications service WhatsApp was a leader in offering consumers robust privacy protections.[44] Soon after its acquisition, Meta degraded privacy protections on WhatsApp, bundling customers' data into their main Meta social network profile.[45]

Since merger enforcement takes a broad review of transactions extending into increased prices, reduced output and quality, or adverse effects on innovation,[46] merger enforcement is particularly well positioned to promote privacy protections. Most importantly, merger enforcement directly prevents increasing market concentration and inhibits the loss of consumer choice.[47] Preventing market concentration has multiple positive effects: averting the loss of competitors, preventing the aggregation of data that can multiply the number of channels to collect it, and ensuring that proper market incentives exist so that competitors can implement privacy protections as a way to differentiate their product quality.[48]

Merger enforcement can also promote privacy protections by imposing strict settlement requirements. Antitrust enforcement agencies have broad authority to structure settlements in the public interest and can impose requirements on merging firms to maintain certain practices that protect user privacy or incur hefty fines or structural breakups.[49]

Antitrust enforcement can also facilitate privacy interests by targeting various methods of monopolization. As described above, privacy protections are a non-price indicator of product quality and can also be an indicator of product innovation. While using the degradation in privacy as the primary means to establish whether the violative conduct produces sufficient adverse effects to show harm to the "competitive process" would be difficult,[50] such a legal avenue is still available and indeed necessary to assert given that many of the products and services at issue are provided for free to users.[51]

Concerning enforcement against deception, while the evidence clearly shows that providing consumers the opportunity to agree to terms of service that detail a firm's privacy policies is woefully ineffective at securing their desire for inhibiting the gathering of their data and

40 See U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines § 1, at 2 (2010). (discussing how antitrust law can analyze price and non-price effects like decreasing quality, reduced service, and declining innovation).

41 H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Administrative Law, 117th Cong., Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations 12 (2022) (hereinafter "House Report").

42 David Millon, *The Sherman Act and the Balance of Power*, 61 S. Cal. L. Rev. 1219, 1264 (1988); Stucke, *supra* note 6, at 288-89.

43 Hanley, *supra* note 16, at 349.

44 FTC Facebook Complaint at 41.

45 *Id.* at 49.

46 John M. Newman, *Antitrust in Zero-Price Markets: Applications*, 94 Wash. U.L. Rev. 49, 58 (2016).

47 See generally Peter C. Carstensen & Robert H. Lande, *The Merger Incipiency Doctrine and the Importance of "Redundant" Competitors*, 2018 Wis. L. Rev. 781 (2018).

48 House Report, *supra* note 41, at 39 ("[In] digital markets…[t]he best evidence of platform market power therefore is not prices charged but rather the degree to which platforms have eroded consumer privacy[.]").

49 See, e.g. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook; *United States v. Am. Tel. & Tel. Co.* (AT&T), 552 F. Supp. 131, 139 (D.D.C. 1982), *aff'd sub nom. Maryland v. United States*, 460 U.S. 1001 (1983) (Breaking up AT&T into seven telephone companies and a long-distance carrier); 15 U.S.C. § 16(e) (requiring settlements entered into by the United States to be in the public interest).

50 *NYNEX Corp. v. Discon, Inc.*, 525 U.S. 128, 135 (1998); Grunes & Stucke, *supra* note 26, at 8-9.

51 Hanley, *supra* note 16, at 279.

making consumers aware of how their data is collected and used,[52] antitrust enforcement can serve as a bulwark to ensure the minimal notice-based protections afforded to consumers are operating (at least to the extent they possibly can) for the benefit of the users.

The bare minimum requirement of proper notice to consumers is that it accurately and meaningfully conveys how their data is being collected and what it is being used for. Since data can provide such significant monopolization capabilities, a firm can easily justify pursuing deception and other nefarious practices on the grounds that short-run legal troubles — such as breach of contract or tarnishment of their brand — are worth the durable and dominant position that can be obtained in the future.[53] Considering the extensive harms caused by deception to consumers and market competition, including the "lack [of] any redeeming economic qualities or cognizable efficiency justifications," such conduct is well within the purview of the antitrust laws.[54]

Third, antitrust enforcement – both through full trials on the merits and through settlements – can pursue, and courts can grant, broad structural remedies that facilitate privacy protections. The federal courts possess remarkably broad remedial authority to address the adverse effects of the litigated antitrust violations to "cure the ill effects of the illegal conduct, and assure the public freedom from its continuance. Such action is not limited to the prohibition of the proven means by which the evil was accomplished, but may range broadly through practices connected with acts actually found to be illegal."[55] Court injunctions can and indeed must be designed to stop the violative conduct, inhibit it from occurring again from both the current and potential violators, and ensure the conditions of a market are conducive to real competition between firms.[56] Such structural remedies can break apart and inhibit the collection and aggregation of user data and create a market that can facilitate privacy interests.

IV. CONCLUSION

As long as technology companies rely on user data as the fundamental basis for their products and services, the rules governing privacy will always be a relevant and necessary discussion. A comprehensive federal law is long overdue in the United States, but federal antitrust enforcers have tools to ensure that in the meantime consumer privacy interests are protected.

52 Stucke, *supra* note 6, at 289.

53 Maurice E. Stucke, *How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?*, 63 SMU L. Rev. 1069, 1087, 1098, 1102 (2010); Note, *Deception as an Antitrust Violation*, 125 Harv. L. Rev. 1235, 1238 (2012) (hereinafter "Deception Note"); *United States v. Microsoft Corp.*, 253 F.3d 34, 76-77 (D.C. Cir. 2001); *McWane, Inc. v. FTC*, 783 F.3d 814, 838 (11th Cir. 2015).

54 Deception Note, *supra* note 53, at 1245-55.

55 *United States v. United States Gypsum Co.*, 340 U.S. 76, 88-89 (1950); see also *California v. Am. Stores Co.*, 495 U.S. 271, 294 (1990) ("[The Clayton Act's injunction provision] should be construed generously and flexibly pursuant to principles of equity").

56 *United States v. Grinnell Corp.*, 384 U.S. 563, 577 (1966) (stating that "adequate relief in a monopolization case should . . . break up or render impotent the monopoly power."); *Nat'l Soc. of Pro. Engineers*, 435 U.S. at 698 (An injunction is judged in part on whether "the relief represents a reasonable method of eliminating the consequences of the illegal conduct."); *United States v. E. I. du Pont de Nemours & Co.*, 366 U.S. 316, 326 (1961) (Relief must "restore competition."); *Ford Motor Co. v United States,* 405 U.S. 562, 575(1972) (The remedy should "cure the ill effects of the illegal conduct[.]") (internal citations omitted).

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.