Notes

The Latest Interface: Using Data Privacy as a Sword and Shield in Antitrust Litigation

SAMMI CHEN[†]

The new and growing intersection between data privacy and antitrust uses data privacy as both a sword and shield against antitrust liability. On one hand, large technology firms have begun using privacy as a business justification for alleged antitrust misconduct. On the other hand, private and government plaintiffs have raised privacy concerns in antitrust litigation. Although antitrust law and data privacy law are two distinct bodies of legal doctrines, there is literature suggesting their consolidation in certain contexts. The Hipster Antitrust movement and integrationist theory purport that data privacy should be included in an antitrust review when privacy is a parameter of a product or service and its quality is affected by competition. Given that data privacy has been a trending factor in antitrust litigation, it is crucial for privacy and antitrust experts to work together in order to comprehend the scope of privacy in antitrust review.

Examples of recent cases that involve the budding intersection between privacy and antitrust, specifically using data privacy as a sword or shield against antitrust liability, include HiQ Labs, Inc. v. LinkedIn Corp.*,* Epic Games, Inc. v. Apple, Inc.*,* Klein v. Facebook, Inc.*, and* United States v. Google LLC*, a majority of which are still pending. As for the aftermath of such litigation, we can expect to see government antitrust regulators beginning to weave privacy into their review and enforcement given President Biden's recent appointments. We should also expect to see courts and judges accepting privacy claims and defenses in antitrust litigation. However, it is unlikely that such litigation will affect large technology firms' corporate practices, especially firms whose business models rely on collecting and selling user data. Though still in an early stage, the nascent intersection between privacy and antitrust can be expected to grow in the following years.*

[†] J.D. Candidate 2023, University of California College of the Law, San Francisco (formerly UC Hastings), Senior Development Editor, *Hastings Law Journal*. I would first like to thank my family and friends for their constant support. I am also grateful to Professor David Rudolph for his guidance and to the editors of the *Hastings Law Journal* for their diligent hard work.

TABLE OF CONTENTS

INTRODUCTION

Upon initial reflection, privacy law and antitrust law appear to be two distinct sets of doctrines with no connection to each other. It is contended that the idea of privacy law was first brought to light in 1890 by Samuel Warren and Louis Brandeis's article, *The Right to Privacy*, in which the authors argue that individuals have the right "to be left alone."[1] Warren and Brandeis were concerned with the emergence of new technology, stating that "[i]nstantaneous photographs . . . have invaded the sacred precincts of private and domestic life,"[2] and asserting the desirability and necessity for the common law to invoke protections for individual privacy.[3] Coincidentally, the same year *The Right to Privacy* was published, and in response to public hostility toward large corporations like the railroad and oil industries monopolizing certain industries, Congress enacted the Sherman Act, the first ever antitrust law.[4] The Act outlaws trusts, monopolies, cartels, and business practices that restrain trade.[5]

Despite this serendipity, the respective histories of privacy and antitrust law could not be more distinct. However, with the emergence of new technologies and innovations, the intersection between privacy and antitrust is becoming evident.[6] Privacy has been defined as a sweeping concept that encompasses "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[7] The concept of data privacy first emerged when the government began collecting census data, telegraph communications, and private mail.[8] But it was the invention of the computer that dramatically altered the way data was collected, disseminated, and used.[9] Data privacy, a subset of the concept of privacy, focuses on "the use and governance of personal data."[10] Enter the age of digital

1. Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

2. *Id.* at 195.

3. *Id.* at 196–97.

4. Sherman Act, ch. 647, 26 Stat. 209 (1890) (codified as amended at 15 U.S.C. §§ 1–7); *see also* Will Kenton, *Sherman Antitrust Act*, INVESTOPEDIA, https://www.investopedia.com/terms/s/sherman-antiturst-act.asp#citation-2 (June 29, 2022).

5. 15 U.S.C. §§ 1–3.

6. *See generally* Erika M. Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (Temple U. Beasley Sch. L. Legal Stud., Rsch. Paper No. 2021-40, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstractid=3880737# (discussing the interactions between antitrust and data privacy law around the world).

7. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).

8. Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 1-6 to -8 (Christopher Wolf ed., 2006).

9. *Id.* at 1-22 to -23.

10. *About the IAPP*, IAPP, https://iapp.org/about/what-is-privacy/ (last visited Jan. 28, 2023).

platforms and Big Tech[11]: both antitrust and data privacy law affect companies that retain and utilize our personal data, and in turn, consumers.[12]

The overlap between antitrust and privacy concerns in technology companies is now glaringly obvious. In August 2020, the House Judiciary Committee's Subcommittee on Antitrust, Commercial, and Administrative Law grilled Amazon, Apple, Facebook, and Google to answer for both their anticompetitive conduct and privacy issues in their data-collection practices.[13] During the six-hour hearing, leaders of the Big Tech companies were questioned about the use of data collection in the furtherance of anticompetitive conduct, such as Facebook's use of surveillance tools to observe competitors and Amazon's use of third-party data to enhance its own product lines.[14]

While Big Tech companies have been accused of exploitative and abusive data privacy practices, there have been some instances in which these companies have used stricter privacy controls to disadvantage competitors.[15] When consumers are provided with a multitude of options as to which platform to use, they may choose their optimal option based on the different qualities or features the platform has to offer, such as their privacy policies. Different companies may offer more or less privacy to their users, which in turn provides users with many different levels of privacy.[16] An early example of using privacy as a form of competition is the former rivalry between Facebook and MySpace.[17] MySpace, a social media platform predating Facebook, made little effort to address privacy concerns.[18] To gain a competitive edge over MySpace, Facebook marketed itself as pro-privacy and promised not to surveil its users for commercial purposes.[19] Another example is Google's proposal to eliminate third-party cookies.[20] The Federal Trade Commission (FTC) deemed Google's plan, which has since been withdrawn, as having anticompetitive intent and effect.[21]

The concept of using stricter privacy controls to curb competitors is not the only way privacy has been used by technology companies to evade alleged

11. "Big Tech" refers to the large technology companies: Facebook, Google (Alphabet), Amazon, Apple, and Microsoft. *See, e.g.*, Matthew Yglesias, *The Push To Break Up Big Tech, Explained*, VOX (May 3, 2019, 8:10 AM), https://www.vox.com/recode/2019/5/3/18520703/big-tech-break-up-explained.

12. Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J.F. 647, 647–48 (2021).

13. Scott Ikeda, *Big Tech Feeling Legislative Heat After Contentious Congressional Hearing on Privacy Issues and Acquisitions*, CPO MAG. (Aug. 10, 2020), https://www.cpomagazine.com/data-privacy/big-tech-feeling-legislative-heat-after-contentious-congressional-hearing-on-privacy-issues-and-acquisitions/.

14. *Id.*

15. LAURA ALEXANDER, PRIVACY AND ANTITRUST AT THE CROSSROADS OF BIG TECH 5 (2021), https://www.antitrustinstitute.org/wp-content/uploads/2021/12/Privacy-Antitrust.pdf.

16. Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009 (2013).

17. 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, 46 (2019).

18. *Id.* at 48.

19. *Id.* at 50.

20. ALEXANDER, *supra* note 15.

21. *Id.*

misconduct. Large technology firms have increasingly used privacy as a shield by using privacy concerns to justify allegedly anticompetitive conduct in antitrust enforcement cases.[22] The first case to consider privacy concerns as a defense to a claim of unfair competition was *hiQ Labs, Inc. v. LinkedIn Corp.*[23] HiQ challenged LinkedIn's privacy policy, alleging that LinkedIn denied it access to publicly available LinkedIn members' profiles, hindering hiQ from accumulating data to sell to its clients.[24] Another prominent case in which a technology company used privacy as a shield against antitrust liability is the ongoing *Epic Games, Inc. v. Apple, Inc.* case,[25] which involves allegations that Apple illegally monopolized app distribution and in-app payments on the iOS App Store.[26] This trend of using privacy concerns as a shield against antitrust's sword may ultimately change how regulators and courts deal with the intersection between privacy and antitrust.

Conversely, there are also recent cases in which plaintiffs have alleged privacy concerns as the animating force in antitrust suits against large technology companies, thus using privacy as a sword in the antitrust context.[27] Commentators have suggested that privacy may play a crucial role in antitrust enforcement against Big Tech and its utilization of user data.[28] Most recently, the Department of Justice (DOJ) and fourteen state attorneys general have accused Google of unlawfully monopolizing general search services, search advertising, and general search-text advertising in ongoing enforcement actions.[29] These enforcement actions allege that search competitors such as DuckDuckGo, which set themselves apart from Google through more protective privacy policies, are blocked from entering the search-services market as a consequence of Google's anticompetitive conduct.[30]

Furthermore, in January 2022, Judge Lucy H. Koh[31] allowed a consumer class-action lawsuit to proceed, which alleged that "Facebook acquired and maintained monopoly power in the Social Network and Social Media Markets

22. Michael Scarborough, David Garcia & Kevin Costello, *Privacy Now Looms Large in Antitrust Enforcement*, LAW360 (Sept. 17, 2021, 5:06 PM), https://www.law360.com/articles/1422517/privacy-now-looms-large-in-antitrust-enforcement.

23. 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019), *cert. granted and judgment vacated*, 141 S. Ct. 2752 (2021).

24. *Id.* at 1103.

25. 559 F. Supp. 3d 898, 898 (N.D. Cal.), *appeal filed*, No. 21-16506 (9th Cir. Sept. 13, 2021), *granting stay*, No. 21-16506, 2021 WL 6755197 (9th Cir. Dec. 8, 2021).

26. *Id.* at 923.

27. Scarborough et al., *supra* note 22.

28. *Id.*

29. *Id.*

30. *Id.*

31. In December 2021, Judge Lucy Koh was confirmed to the U.S. Court of Appeals for the Ninth Circuit but has temporarily kept case assignments in the U.S. District Court for the Northern District of California. Press Release, U.S. Cts. for the Ninth Cir., Senate Confirms Judge Lucy Haeran Koh to Seat on U.S. Court of Appeals for the Ninth Circuit (Dec. 14, 2021), https://cdn.ca9.uscourts.gov/datastore/ce9/2021/12/Koh_Lucy_Confirmed.pdf.

by making false representations to users about [its] data privacy practices."[32] How courts will rule on these matters may drastically affect the viability of consumer class-action antitrust claims in the near future. In turn, this could have a severe effect on how Big Tech companies approach data privacy protection on their platforms and how they elect to use their users' data.

Privacy is increasingly used as a justification to defend against allegedly anticompetitive conduct and as an element of product quality that can be diminished by such anticompetitive conduct.[33] Privacy and antitrust agencies must collaborate to fully comprehend this trend and how it affects consumer data protection. The integration of privacy in antitrust review will promote not only competition, but also the protection of consumer data.

To explain how using privacy as both a shield and sword in antitrust litigation will affect the antitrust and privacy legal landscape, this Note proceeds in five parts. Part I provides an overview of antitrust and privacy law in the United States. Part II discusses the intersection between antitrust and privacy in depth, including a theoretical and practical analysis of the two bodies of law. Part III analyzes how defendant technology giants have recently started to use privacy as a sword in antitrust litigation, using privacy concerns to justify anticompetitive conduct. Part IV examines how plaintiffs have started to use privacy as an antitrust-misconduct shield by forwarding a theory that company misuse of user data stifles competition. Part V considers the consequences of using privacy as both a sword and shield to antitrust.

I. DATA PRIVACY AND ANTITRUST LAW

To fully grasp the use of data privacy as both a shield and sword in the antitrust context, it is important to first understand the application and nuances of privacy and antitrust laws in the United States. This Part provides an overview of current privacy and antitrust laws and their application in private rights of action and government enforcement actions, including the requirements needed to prevail in a data privacy violation claim and an antitrust claim.

A. DATA PRIVACY LAW AND LITIGATION

In the United States, there is no singular federal law or uniform scheme that covers data privacy; rather, there is a mix of laws that protect specific types of data, such as the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act.[34] Since there is no single preemptive federal data privacy protection law, states may impose and enforce their own data protection laws to protect their citizens as well.[35] In most

32. Klein v. Facebook, Inc., 580 F. Supp. 3d 743, 763 (N.D. Cal. 2022).

33. Scarborough et al., *supra* note 22.

34. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

35. *Id.*

states, companies may use, share, or sell any data they collect without notification or consent from users.[36] Many states do not require user notification of company data breaches or the sale of sensitive consumer data.[37] As of 2022, only five states have comprehensive consumer privacy laws: California, Virginia, Colorado, Connecticut, and Utah.[38] The laws in these states have provisions that allow consumers to control their data by requiring companies to notify users about the sale of and right to access, delete, or correct their data.[39] Only state residents are entitled to these data privacy rights under their respective state's statutes.[40]

1. Private Rights of Action

There is also currently no single federal law that provides a private right of action allowing individuals to sue companies directly for privacy violations. Instead, there are limited state and federal laws that provide private rights of action in various areas of the law.[41] When consumers do not have the option of exercising a private right of action, they must rely on federal or state enforcers to protect their privacy.[42] On one hand, commentators argue that private rights of action are fundamental to democracy, as the ability of an individual to bring a lawsuit against another party who has harmed them is the premise of the American judicial system.[43] On the other hand, many industry representatives argue that private rights of action lead to nuisance lawsuits regardless of their merits, and that agency enforcement is more productive than private litigation.[44] State and federal laws that grant private rights of action have frequently been the basis for consumer class-action claims.[45]

California arguably has the strongest privacy protections in the country, for several reasons. For example, the California Consumer Privacy Act (CCPA)

---

36. *Id.*

37. *Id.*

38. *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others.

39. Klosowski, *supra* note 34.

40. *Id.*

41. BECKY CHAO, ERIC NULL & CLAIRE PARK, ENFORCING A NEW PRIVACY LAW: WHO SHOULD HOLD COMPANIES ACCOUNTABLE? 16 (2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/.

42. *Id.*

43. *Id.*

44. *See* Cameron F. Kerry & John B. Morris, *In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition*, BROOKINGS (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/; *see also* Melissa Bianchi, Mark W. Brennan, Adam Cooke, Joseph Cavanaugh & Alicia Paller, *Ill Suited: Private Rights of Action and Privacy Claims*, HOGAN LOVELLS (July 19, 2019), https://www.engage.hoganlovells.com/knowledgeservices/news/ill-suited-private-rights-of-action-and-privacy-claims.

45. Cathy Cosgrove, *Standing Issues in U.S. Privacy Class Actions*, IAPP (Aug. 24, 2021), https://iapp.org/news/a/standing-issues-in-u-s-privacy-class-actions/#:~:text=While%20there%20is%20no%20federal,basis%20for%20class%20action%20claims.

includes a limited private right of action for data breaches.[46] Section 1798.150(a)(1) of the CCPA permits a private right of action to

> any consumer whose non-redacted personal information . . . is subject to unauthorized access and exfiltration, theft, or disclosure [i.e., data breach] as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.[47]

Under section 1798.81.5(d)(1)(A), personal information is defined as "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements," such as a social security number, driver's license number, passport number, bank account number, medical information, health insurance information, unique biometric data, or genetic data.[48] The statutory damages available for a private right of action range from $100 to $750 per consumer incident or actual damages, whichever is greater.[49] The prevailing party may also seek injunctive or declaratory relief, or any other relief the court deems proper.[50]

Another comprehensive state law that provides consumers with a private right of action is the Illinois Biometric Information Privacy Act (BIPA).[51] Section 14/20 states that "[a]ny person aggrieved by a violation of this Act shall have a right of action . . . against an offending party."[52] A prevailing party may recover against a private entity that negligently violates BIPA for liquidated damages of $1,000 or actual damages, whichever is greater.[53] The prevailing party may also recover against a private entity that intentionally or recklessly violates a provision of BIPA for liquidated damages of $5,000 or actual damages, whichever is greater.[54] The prevailing party may also be granted other relief, such as an injunction, if the court deems it appropriate.[55]

Again, there is no single comprehensive federal law that provides individuals with a private right of action to directly sue companies for privacy violations.[56] Instead, there are certain federal privacy laws that authorize private rights of action, such as the Fair Credit Reporting Act, the Privacy Act, the Right to Financial Privacy Act, the Cable Communications Policy Act, the Electronic

46. Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, IAPP (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/.

47. CAL. CIV. CODE § 1798.150(a)(1) (West 2022).

48. *Id.* § 1798.81.5(d)(1)(A).

49. *Id.* § 1798.150(a)(1)(A).

50. *Id.* § 1798.150(a)(1)(B)–(C).

51. 740 ILL. COMP. STAT. 14/20 (2008).

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. Kerry & Morris, *supra* note 44.

Communications Privacy Act, the Video Privacy Protection Act, and the Telephone Consumer Protection Act.[57]

It is important to note that although certain state and federal laws do not provide a private right of action for privacy claims, plaintiffs may still prevail in a privacy suit on other claims, such as on a tort, contract, or constitutional claim. For example, there have been privacy cases in which plaintiffs have brought claims for intrusion upon seclusion, negligence, breach of contract, breach of implied covenant of good faith and fair dealing, restitution, and unjust enrichment.[58]

2. Standing Requirements

While federal and state privacy laws, along with tort and contract claims, have been the basis for many class actions, a difficult hurdle for plaintiffs in privacy cases is meeting the threshold standing requirements necessary to sue.[59] It is difficult for plaintiffs to satisfy standing in privacy suits, since they often allege intangible and future harms as the injury.[60] In *Lujan v. Defenders of Wildlife*, the Supreme Court set forth a three-prong test to determine whether a party has Article III standing to sue: (1) the plaintiff must have suffered an "injury in fact," meaning that the injury is of a legally protected interest that is (a) concrete and particularized and (b) actual or imminent; (2) the injury must be fairly traceable to the challenged action of the defendant; and (3) it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision of the court.[61] Defendants commonly challenge privacy claims on the grounds that plaintiffs have not suffered an "injury," which is a prerequisite to bring suit.[62] In two subsequent Fair Credit Reporting Act cases, *Spokeo v. Robins*[63] and *TransUnion LLC v. Ramirez*,[64] the Supreme Court clarified that "standing requires a concrete injury even in context of statutory violations and [that] alleging a bare procedural violation" does not pass muster.[65]

57. *Id.*

58. *See generally In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020), *cert. denied sub nom.* Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021) (asserting claims of breach of contract, breach of implied covenant of good faith and fair dealing, and intrusion upon seclusion and invasion of privacy); Calhoun v. Google LLC, 526 F. Supp. 3d 605 (N.D. Cal. 2021) (asserting claims of invasion of privacy, intrusion upon seclusion, breach of contract, breach of implied covenant of good faith and fair dealing, restitution and unjust enrichment, and statutory larceny); *In re* TikTok, Inc. Consumer Priv. Litig., No. 20 C 4699, 2022 WL 2982782 (N.D. Ill. July 28) (asserting claims of violation of right to privacy under the California Constitution, intrusion upon seclusion, negligence, and restitution and unjust enrichment), *appeal filed*, No. 22-2682 (7th Cir. Sept. 21, 2022).

59. Cosgrove, *supra* note 45.

60. *Id.*

61. 504 U.S. 555, 560–61 (1992).

62. Cosgrove, *supra* note 45.

63. 578 U.S. 330 (2016).

64. 141 S. Ct. 2190 (2021).

65. Cosgrove, *supra* note 45.

As a result, courts must determine whether injuries in privacy lawsuits are sufficiently "concrete" or "imminent" to satisfy standing.

The difficulty of establishing standing in privacy litigation turns on what constitutes a sufficiently "concrete" injury under *Spokeo* and now *Ramirez*. However, courts have started articulating clearer foundations for standing. Recently, in *In re Facebook, Inc. Internet Tracking Litigation*, the Ninth Circuit held that plaintiffs adequately established standing for their statutory and common-law privacy claims by "alleg[ing] that Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information."[66] The Ninth Circuit also held that "Facebook's monetization of improperly collected user data can constitute an economic injury, namely unjust enrichment, allowing plaintiffs to establish standing on several state law claims."[67] These holdings set an important precedent for determining plaintiffs' Article III standing in future privacy litigation.

B. ANTITRUST LAW AND LITIGATION

There are three core federal antitrust laws in the United States: the Sherman Act, the Federal Trade Commission Act, and the Clayton Act.[68] Section 1 of the Sherman Act states: "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce . . . is declared to be illegal."[69] Section 2 of the Sherman Act further provides: "Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of trade or commerce . . . shall be deemed guilty of a felony."[70] Furthermore, the Supreme Court has ruled that not every restraint on trade is illegal, only those that are unreasonable.[71] In sum, the purpose of the Sherman Act is to "promote economic fairness and competitiveness"[72] by outlawing monopolies and anticompetitive agreements.

The Federal Trade Commission Act outlaws "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[73] The Act also creates the FTC.[74] The Supreme Court

66. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 599 (9th Cir. 2020), *cert. denied sub nom.* Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021); *see* Wyatt Larkin, *The Ninth Circuit Facebook Case That May Shape the Future of Privacy Litigation: In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020)*, BERKELEY TECH. L.J. (Dec. 1, 2020), https://btlj.org/2020/12/the-ninth-circuit-facebook-case-that-may-shape-the-future-of-privacy-litigation-in-re-facebook-inc-internet-tracking-litig-956-f-3d-589-9th-cir-2020/.

67. Larkin, *supra* note 66; *In re Facebook*, 956 F.3d at 599–600.

68. *The Antitrust Laws*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws (last visited Jan. 28, 2023).

69. 15 U.S.C. § 1.

70. *Id.* § 2.

71. *The Antitrust Laws*, *supra* note 68.

72. Kenton, *supra* note 4.

73. 15 U.S.C. § 45.

74. *The Antitrust Laws*, *supra* note 68.

has ruled that all violations of the Sherman Act are also violations of the Federal Trade Commission Act.[75] Although the FTC does not technically enforce the Sherman Act, under the Federal Trade Commission Act, the FTC can bring cases against the same kind of activities that violate the Sherman Act.[76] The FTC is also the only agency or party that can bring cases under the Federal Trade Commission Act.[77]

On the other hand, the Clayton Act allows for a private right of action for conduct that violates the Sherman or Clayton Act.[78] The Clayton Act outlaws mergers and acquisitions that "may be substantially to lessen competition, or to tend to create a monopoly,"[79] and was intended to strengthen earlier antitrust legislation. The Clayton Act also prohibits discriminatory and predatory pricing in dealings between merchants and requires companies planning large mergers or acquisitions to notify the government.[80]

As for enforcement, private parties, usually businesses and individuals, may seek damages or injunctive relief under the Sherman or Clayton Act, or under state antitrust laws.[81] To bring a private right of action under federal antitrust laws, an antitrust claimant must have Article III standing in addition to demonstrating an antitrust injury and antitrust standing.[82] An antitrust injury "requires the claimant to allege harm to competition (not just harm unique to the claimant) and which is the type of harm the antitrust laws were intended to prevent."[83] In *Brunswick v. Pueblo Bowl-O-Mat, Inc.*, the Supreme Court stated that the purpose of antitrust laws is the protection of competition, not competitors.[84] "Antitrust standing is [also] limited to consumers and competitors in the relevant market and injuries that are 'inextricably intertwined' with the alleged harmful conduct."[85] If the antitrust claim was directly targeted and the harm was "the essential component of the [defendant's] anticompetitive scheme as opposed to . . . an ancillary byproduct of it," the injury is considered "inextricably intertwined" with the alleged harmful conduct.[86] In addition, an antitrust claimant must "provide sufficient facts to plausibly state that a violation

75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. 15 U.S.C. § 18.
80. *The Antitrust Laws*, *supra* note 68.
81. *The Enforcers*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers (last visited Jan. 28, 2023).
82. Paul H. Saint-Antoine, Joanne C. Lewers, Lee Roach, Lucas B. Michelen, John S. Yi & Amanda M. Pasquini, *Private Antitrust Litigation in the United States: Overview*, WESTLAW, https://www.westlaw.com/6-632-8692?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 (last visited Jan. 28, 2023).
83. *Id.*
84. 429 U.S. 477, 488 (1977).
85. Saint-Antoine et al., *supra* note 82.
86. *Id.*

of the antitrust laws has occurred," which heavily depends on the nature of the specific antitrust claim asserted.[87]

State attorneys general may also bring federal antitrust suits on behalf of the state or individuals residing within their states, or an action to enforce the state's antitrust laws.[88] For the federal government, both the FTC and DOJ can enforce federal antitrust statutes.[89] Generally, during an FTC investigation, if the FTC believes a company or person has violated antitrust laws or that a proposed merger would violate the law, the FTC or DOJ can attempt to obtain voluntary compliance by entering into a "consent order" with the company.[90] A consent order allows the company or individual to agree to stop the challenged practices or to take certain steps to resolve the anticompetitive aspects of a merger or acquisition without admitting to a violation of the law.[91] If the consent order or agreement is not attained, however, the FTC may issue an administrative complaint, resulting in a formal proceeding before an administrative law judge, or seek injunctive relief in federal court.[92] With the submission of evidence and testimonies and witness examination and cross-examination, the administrative proceeding is similar to a federal court trial.[93] Initial decisions by the administrative law judge may be appealed to the Commission, and final decisions may be appealed to a U.S. Court of Appeals and the Supreme Court.[94] Under certain circumstances, such as for effective merger enforcement, the FTC may seek consumer redress, civil penalties, or an injunction directly in federal court.[95]

II. INTERSECTION BETWEEN PRIVACY AND ANTITRUST

Much of the existing literature touching on the intersection between privacy and antitrust suggests that while privacy and antitrust may be complementary, they are still distinct areas of the law.[96] However, given recent developments in Big Tech and consumer data privacy concerns, some recent literature has suggested the opposite—that the relationship between privacy and antitrust is more than just complementary.[97] There are two commonly articulated theories about the interaction between antitrust and data privacy.[98] First, the

87. *Id.*
88. *The Enforcers*, *supra* note 81.
89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1130 (2016).
97. *See generally* Douglas, *supra* note 6; Srinivasan, *supra* note 17.
98. Douglas, *supra* note 12, at 651.

"separatist" theory advocates for the doctrinal separation between data privacy and antitrust law.[99] It also emphasizes the separation between the FTC's competition and consumer protection mandates.[100] The separatist theory argues that the two separate areas of law address distinct legal harms, where antitrust law is used to address conduct harmful to consumer welfare or economic competition while data privacy protects consumers' informed choice and reasonable consumer expectations.[101] Alternatively, the "integrationist" theory argues that an antitrust analysis must consider data privacy when it is an element of quality-based competition.[102] The integrationist theory starts from the position that "consumer welfare is improved by competition that is based not only on price, but also non-price factors, like quality" and interprets "quality" to include privacy-based competition.[103] Between the two theories, the integrationist theory has become the most accepted view on the intersection between antitrust and data privacy, with the FTC and DOJ adopting and applying it in merger cases.[104]

In light of the recent tension between antitrust and data privacy, this Part examines the integrationist theory in depth and its practicality in the real world. Antitrust and data privacy analyses are at the forefront when discussing digital information and platforms like Big Tech. Although some scholars have advocated for the distinction between antitrust and data privacy, there is no denying that the two are intertwined, considering how Big Tech companies have used privacy controls to curb competitors or, more recently, justify anticompetitive conduct, and how plaintiffs have wielded privacy concerns in antitrust complaints.[105] When privacy is the framework for a product or platform, antitrust and data privacy laws are more than just complementary; they become integrated.

A. THE HIPSTER ANTITRUST MOVEMENT

One example of a campaign that incorporates data privacy into antitrust analysis is the Hipster Antitrust movement. The Hipster Antitrust movement, also known as the New Brandeis movement, promotes a broader view of the harms caused by giant corporations[106] and seeks to "overturn the established consumer welfare standard that is guided by price theory analysis."[107] The

99. *Id.* at 653.
100. *Id.*
101. *Id.*
102. *Id.* at 654.
103. *Id.*
104. *Id.* at 655.
105. *See supra* p. 557.
106. Gina Chon, *Breakdown: Antitrust's Hipsters Go Mainstream*, REUTERS, https://www.reuters.com/article/us-usa-antitrust-breakingviews/breakdown-antitrusts-hipsters-go-mainstream-idUSKBN2B3016 (Mar. 10, 2021, 4:24 PM).
107. Andrea O'Sullivan, *What Is 'Hipster Antitrust?,'* MERCATUS CTR. (Oct. 18, 2018), https://www.mercatus.org/bridge/commentary/what-hipster-antitrust.

movement has been branded the New Brandeis movement as a nod to Justice Brandeis, a former Supreme Court Justice who was a strong advocate of democratic distribution of power and opportunity in the political economy, especially during America's antimonopoly regime in the industrial era.[108] The Hipster Antitrust movement seeks to address how giant corporations' actions impact socioeconomic problems such as low wages and unemployment.[109] Opponents of the movement, such as former Senator Orrin Hatch, argue that the movement lacks economic analysis and broadly views big corporations as bad actors without actual evidence.[110] In opposition, supporters of the movement, most notably Lina Khan, the current Chair of the FTC, claim that the consumer welfare standard falls short, and that monopoly pricing paid by consumers benefits giant corporations and contributes to the wealth of the one percent.[111]

The Hipster Antitrust movement also accounts for the significance of data and network effects in deals.[112] The ability to quantify the amount of data and network of Big Tech companies allows for a more effective enforcement of antitrust laws in the technology space.[113] Network effects of technology companies become more valuable as more users choose to use their platforms, and companies such as Facebook and Amazon suddenly become "gatekeepers that other companies must please to get access to those customers,"[114] which in turn increases their market dominance. The movement also scrutinizes Big Tech companies' market dominance and its effects on consumers. For example, even though Facebook became one of the leading social media companies in the world by providing free membership, Facebook harms its users by misusing their data, as evidenced by incidents like the Cambridge Analytica scandal.[115]

In an American Productivity & Quality Center podcast, hosts Lauren Trees and Carla O'Dell discuss how the Hipster Antitrust movement and Lina Khan's focus on data privacy will affect knowledge management.[116] The hosts argue for a broader definition of antitrust that includes an analysis of how consumer data is collected and used, and how it may affect how companies handle data as consumers and employees begin to become more aware of the data that is being collected.[117] They also argue that if the movement progresses, disclosure will

108. Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. EUR. COMPET. L. & PRAC. 131, 131 (2018).

109. Chon, *supra* note 106.

110. *Id.*

111. *Id.*

112. Kevin Yeh, *Hipster Antitrust*, AM. BAR ASS'N, https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/antitrust/hipster-antitrust-brief-primer/ (last visited Jan. 28, 2023).

113. *Id.*

114. Chon, *supra* note 106.

115. *Id.*

116. *Why "Hipster Antitrust" Matters for Knowledge Management*, APQC PODCASTS, at 02:00 (Sept. 29, 2021) (downloaded using APQC Podcasts).

117. *Id.* at 01:42.

become more crucial because companies may have to be more transparent about the data profiles they collect.[118]

Given Lina Khan's confirmation to the FTC and her support of the Hipster Antitrust movement, it is likely that a data privacy analysis may become integrated into antitrust review or enforcement. In sum, the movement provides just another example of how antitrust and privacy concerns are intertwined and highlights the importance of viewing them together in the context of Big Tech.

B. INTEGRATIONIST ("PRIVACY AS QUALITY") THEORY

At a high level, both data privacy and antitrust laws attempt to benefit consumers and their interests. Data privacy and antitrust laws also seek to enforce consumer trust and maintain consumer choice in markets.[119] The integrationist theory, also known as "privacy as quality" theory, is the leading theory on the intersection of antitrust and data privacy. Under this theory, an antitrust analysis should be implemented when, and only when, "privacy is a parameter of product (or service) quality that is affected by competition."[120] An application of this theory is when companies compete to offer more protective privacy settings or less collection of personal data.[121] For example, one of Google's competitors, DuckDuckGo, distinguishes its product from Google by offering a more privacy-protective search engine.[122] DuckDuckGo's business model promises its users not to collect personal data, keeps searches private and anonymous, and offers built-in blocking so that websites have a more difficult time collecting user data.[123] Under the integrationist theory, if DuckDuckGo and another internet browser company that also offers user privacy–protective features were to merge, the transaction might reduce the level of competition in the internet browser market to offer such features. If the reduction in competition would cause a decline in user privacy protection in the internet browser industry, the antitrust analysis of the merger would account for the effect on privacy-related quality.[124]

Another application of this theory is where anticompetitive conduct of a dominant firm results in a reduction in privacy-related competition and quality.[125] In October 2020, the Antitrust Division of the DOJ alleged exactly

118. *Id.* at 07:35.

119. Douglas, *supra* note 6, at 6–7.

120. *Id.* at 7.

121. *Id.*

122. Adam Benjamin, *DuckDuckGo: What To Know About the Privacy-Focused Search Engine*, CNET (Aug. 10, 2022, 2:15 AM), https://www.cnet.com/tech/services-and-software/duckduckgo-what-to-know-about-the-privacy-focused-search-engine/.

123. *Id.*

124. Douglas, *supra* note 6, at 7–8.

125. *Id.* at 8.

this in a monopolization complaint against Google.[126] In a public press release, the DOJ named Google as a monopoly gatekeeper to the internet for billions of users and advertisers worldwide, citing that Google accounted for ninety percent of all search queries in the United States.[127] The DOJ alleged that Google has unlawfully maintained monopolies in the search and search-advertising industries by "[e]ntering into exclusivity agreements that forbid preinstallation of any competing search service"; "[e]ntering into tying and other arrangements that force preinstallation of its search applications in prime locations on mobile devices"; "[e]ntering into long-term agreements with Apple that require Google to be the default and *de facto* exclusive[] general search engine on Apple's popular Safari browser and other Apple search tools"; and "[g]enerally using monopoly profits to buy preferential treatment for its search engine on devices, web browsers, and other search access points, creating a continuous and self-reinforcing cycle of monopolization."[128] The DOJ then argued that Google's conduct, which restricts competition in the search market, has harmed consumers by reducing the quality of search, including features in privacy; data protection; and use of consumer data, which in turn lessens consumer choice.[129] Google's conduct is a perfect example of how privacy has become a product quality that has diminished due to the company's anticompetitive behavior.

In reverse, antitrust analysis would view a potential merger or company misconduct that has the effect of increasing privacy quality through competition as a positive effect.[130] Nevertheless, practices that improve privacy but violate antitrust law create a conflict between the two areas of law, raising new questions of how to handle such matters. For example, both antitrust and data privacy agencies have been watching closely as Google plans to phase out third-party tracking cookies from its Chrome internet browser.[131] U.S. state attorneys general have filed a joint complaint against Google, alleging that although blocking cookies might be a positive thing for consumers, because Chrome dominates the browser market, Google's plan would only make its own advertising system more attractive to advertisers.[132] Similarly, the Electronic Frontier Foundation, a pro-privacy organization, has criticized Google's conduct as self-serving, as it would put the Chrome browser at the center of tracking and targeting in the advertisement space.[133] This illustrates how firm practices that

126. Press Release, U.S. Dep't of Just., Justice Department Sues Monopolist Google for Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

127. *Id.*

128. *Id.*

129. *Id.*

130. Douglas, *supra* note 6, at 8.

131. *Id.* at 16.

132. Adi Robertson & Russell Brandom, *Google Antitrust Suit Takes Aim at Chrome's Privacy Sandbox*, THE VERGE (Mar. 16, 2021, 8:50 AM), https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy.

133. *Id.*

improve privacy protections while violating antitrust laws raise new questions on how to scrutinize and remedy the conflict.

Although the integrationist theory is the leading perspective on the intersection between data privacy and antitrust, its potential implications are still at an early stage of development.[134] Most of its applications are in merger reviews for antitrust analysis of privacy-based competition, with rare applications in abuse of dominance cases.[135] Antitrust enforcers and investigators analyze certain evidence to determine whether data privacy is the basis for competition, including:

> consumer and competitor surveys on whether data privacy is a driver of competition, observations of privacy-related market behavior (for example, whether competing companies change their privacy policies in response to one other) and internal company documents (for example, to provide insight on why a company made changes to its privacy policy).[136]

Although this type of evidence is helpful in determining whether privacy is the basis for competition, there is no set analytical approach for this assessment.[137] The lack of a standard for such analysis is a barrier to the integration of privacy into antitrust analysis, but at the same time it provides an opportunity for data privacy and antitrust authorities to develop a standard methodology for measuring competition-related effects on privacy quality.[138]

The practicality of the integrationist theory is still in its early stages of development and requires more examination from privacy and antitrust authorities. Given the recent cases in which Big Tech companies have used privacy to justify anticompetitive conduct and consumers and antitrust enforcers have used privacy concerns in antitrust complaints,[139] data privacy will likely become more relevant in abuse of dominance cases and in claims where data privacy is used as a business justification. As more of these cases develop and as the Hipster Antitrust movement gains more traction, the integration of data privacy and antitrust is inevitable. Antitrust and data privacy authorities must collaborate to determine not only a methodology for measuring privacy competition effects on privacy quality, but also a foundational basis of the scope of protected privacy interests and harms in relation to an antitrust analysis. The combination of antitrust and privacy expertise will lead to a more robust application of the integrationist theory that will in turn reveal more of the comprehensive implications of the relationship between antitrust and data privacy, especially in regard to Big Tech.

---

134. Douglas, *supra* note 6, at 8.
135. *Id.*
136. *Id.* at 9.
137. *Id.*
138. *Id.* at 10.
139. *See infra* Parts III–IV.

III. PRIVACY AS SHIELD

"Antitrust law has not yet determined whether data privacy protection could constitute a procompetitive justification for conduct that would otherwise violate prohibitions on abuse of dominance."[140] However, antitrust policy and cases have begun discussing whether a company may use consumer data privacy protection to justify otherwise anticompetitive conduct.[141] In an antitrust abuse of dominance case, the conduct of the firm is analyzed using a burden-shifting framework.[142] The plaintiff must first establish a prima facie case showing that the defendant's conduct has anticompetitive effects.[143] Once established, the burden shifts to the defendant, who may prove that there is a procompetitive, efficiency-based justification for the alleged misconduct.[144] Usually, the justifications involve showing that there is an economic benefit to consumers.[145] If the plaintiff has no rebuttal or the procompetitive benefits of the alleged misconduct outweighs its anticompetitive effects, then there is no antitrust violation.[146]

In the last five years, there have been several antitrust cases in which Big Tech companies have asserted data privacy protections as a justification for allegedly anticompetitive conduct.[147] Given this recent trend, this Part examines a number of these cases and analyzes the defense arguments, along with the aftermath of such litigation.

A. *HIQ LABS, INC. V. LINKEDIN CORP.*

One of the very first cases in which a court considered privacy concerns as a defense to allegedly unfair competition misconduct is *hiQ Labs*.[148] LinkedIn is a professional networking site with over 500 million members that allows members to post resumes, job listings, and build professional connections with other members.[149] LinkedIn also claims that the information its users post on their profiles is their own, and that the company is only granted a nonexclusive license to "'use, copy, modify, distribute, publish, and process' that information" under the LinkedIn User Agreement.[150] LinkedIn users are allowed to choose their privacy settings, which includes specifying which portions of their profiles are visible to the general public.[151] To protect its platform, LinkedIn also deploys

140. Douglas, *supra* note 6, at 17.
141. *Id.*
142. *Id.* at 126.
143. *Id.*
144. *Id.*
145. *Id.* at 126–27.
146. *Id.* at 127.
147. *Id.*
148. *See generally* 938 F.3d 985 (9th Cir. 2019), *aff'g* 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *cert. granted and judgment vacated*, 141 S. Ct. 2752 (2021).
149. *Id.* at 989.
150. *Id.* at 990.
151. *Id.*

technological systems to protect the data on its website from what it considers misuse or misappropriation.[152]

HiQ Labs is a data analytics company that uses automated bots to scrape information that LinkedIn users include on their *public* profiles, including their name, job title, work history, and skills.[153] HiQ then uses that information with its proprietary algorithm to produce "people analytics" to sell to business clients.[154] In May 2017, LinkedIn sent hiQ a cease and desist letter, asserting that hiQ violated LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's servers.[155] The letter stated that continuing such conduct would constitute violations of state and federal law.[156] In response, hiQ filed suit against LinkedIn, seeking injunctive relief under California law and a declaratory judgment that LinkedIn could not lawfully invoke the Computer Fraud and Abuse Act, Digital Millennium Copyright Act, California Penal Code section 502(c), and the California common law of trespass.[157] The district court granted hiQ's motion, ordering LinkedIn to withdraw its cease and desist letter, remove any existing technical barrier to hiQ's access to public LinkedIn profiles, and refrain from placing any measures with the effect of blocking such access.[158]

The Ninth Circuit affirmed the preliminary injunction, reasoning that hiQ had sufficiently asserted that "the survival of its business [wa]s threatened absent a preliminary injunction" because its business model heavily depended on access to publicly available data.[159] LinkedIn, on the other hand, attempted to argue that the injunction "threaten[ed] its members' privacy and therefore put[] at risk the goodwill LinkedIn . . . developed with its members."[160] LinkedIn also pointed out that more than fifty million members opted for the "Do Not Broadcast" feature to ensure that other users are not notified when the member changes their profile.[161] According to LinkedIn, the popularity of this feature implies that many members, including those who choose to share their information publicly, do not want their current employers to know they may be searching for a new job.[162]

Nevertheless, the Ninth Circuit determined that the district court had not abused its discretion in rejecting LinkedIn's defense on the preliminary injunction record. First, there was insufficient evidence to prove that "LinkedIn users who choose to make their profiles public actually maintain an expectation

152. *Id.*
153. *Id.* at 991.
154. *Id.*
155. *Id.* at 992.
156. *Id.*
157. *Id.*
158. *Id.*
159. *Id.* at 993–94.
160. *Id.* at 994.
161. *Id.*
162. *Id.*

of privacy with respect to the information that they post publicly," given that LinkedIn's privacy policy states that "[a]ny information you put on your profile and any content you post on LinkedIn may be seen by others" and instructs users not to "post or add personal data to your profile that you would not want to be public."[163] Second, there was also insufficient evidence to prove that users who select the "Do Not Broadcast" feature do so exclusively to prevent their employers from being alerted,[164] rather than for other reasons, such as avoiding annoying notifications each time their profile changes.[165] Lastly, the court reasoned that LinkedIn's own conduct contradicted its argument that users have an expectation of privacy.[166] LinkedIn's "Recruiter" feature allows recruiters to "follow" prospects, get alerted when prospects change their profiles, and use those alerts to reach out at just the right moment without the prospect's consent.[167] Accordingly, the Ninth Circuit affirmed the district court's determination that LinkedIn's interests in preventing hiQ from scraping profile data were not significant enough to outweigh hiQ's interest in continuing its business, which heavily depends on accessing information from public LinkedIn profiles.[168]

After establishing that the balance of hardship tilted in hiQ's favor, the Ninth Circuit assessed the merits of hiQ's tortious interference with contract claim under California's Unfair Competition Law (UCL).[169] The court determined that selectively banning potential competitors from accessing and using public data can be considered unfair competition under California law.[170] The court ultimately did not reach hiQ's unfair competition claim, however, concluding that hiQ "ha[d] raised at least serious questions going to the merits of its tortious interference with contract claim" and remanding the claim.[171] It is important to note that the Ninth Circuit's ruling, excluding competitors from accessing and using data that is publicly available, may have serious implications for antitrust laws and large technology firms.

Finally, LinkedIn attempted to argue that the preliminary injunction was against the public interest "because it w[ould] invite malicious actors to access LinkedIn's computers and attack its servers."[172] The Ninth Circuit rejected this argument, noting that the injunction did not prevent LinkedIn from engaging in "technological self-help" against bad actors, such as employing anti-bot measures.[173]

163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.* at 994–95.
167. *Id.* at 995.
168. *Id.*
169. *Id.*
170. *Id.* at 998.
171. *Id.* at 999, 1005.
172. *Id.* at 1005.
173. *Id.*

However, in June 2021, the Supreme Court granted certiorari and issued a summary disposition vacating the Ninth Circuit's judgment and remanding the case for additional consideration in light of *Van Buren v. United States*,[174] a case limiting the reach of the Computer Fraud and Abuse Act (CFAA).[175] In *Van Buren*, the Court ruled that under the CFAA, an individual exceeds "authorized access" when accessing a computer with authorization to obtain information that is off-limits.[176] In LinkedIn's petition for certiorari, it argued that although some of its profiles are public, hiQ's software harvests data on a larger scale than any human could, and therefore urged the Court to clarify the distinction between exceeding authorized access and a private company's ability to deny access altogether.[177]

On remand in April 2022, the Ninth Circuit held that the decision in *Van Buren* reinforced its prior holding and once again affirmed the preliminary injunction.[178] The court held once again that data scraping public websites is not unlawful, and that plaintiffs may not rely on the CFAA to prevent third parties from scraping data from their public websites.[179] The court reasoned that accessing publicly available data cannot violate the CFAA because there are no rules or access permissions that prevent such access.[180]

HiQ Labs is an example of a case in which a technology company failed to assert consumer data privacy protections as a defense to anticompetitive behavior. LinkedIn, a networking company owned by Microsoft, makes its profits by selling user data to employers and recruiters. LinkedIn's Privacy Policy states: "We will share your personal data with our affiliates to provide and develop our Services."[181] LinkedIn viewed hiQ as a competitor in the data-selling market and had a vested interest in protecting its data from rivals, as it is the norm for tech companies to rely on consumer data to compete in the market. It is no surprise that LinkedIn's weak pro-privacy argument failed, given that its own conduct contradicted its defense. But this raises the question of who best represents users' interests. On one hand, LinkedIn has a duty to protect its users' data and to prevent bad actors from accessing such data. On the other hand, if LinkedIn had prevailed in its position of having full control of its publicly available data, including the option to exclude competitors from accessing such

174. 141 S. Ct. 1648, 1662 (2021).

175. LinkedIn Corp. v. hiQ Labs, Inc., 141 S. Ct. 2752 (2021), *vacating* 938 F.3d 985 (9th Cir. 2019).

176. *Van Buren*, 141 S. Ct. at 1662.

177. Mark P. Kesslen, Kathleen A. McGee & Bryan Sterba, *Supreme Court Grants Certiorari in Web Scraping Case HiQ v. LinkedIn*, LOWENSTEIN SANDLER (June 15, 2021), https://www.lowenstein.com/news-insights/publications/client-alerts/supreme-court-grants-certiorari-in-web-scraping-case-hiq-v-linkedin-tech-groupwhite-collar.

178. Jennifer Oliver, *Ninth Circuit Holds Data Scraping Is Legal in HiQ v. LinkedIn*, CAL. LAWS. ASS'N (May 2022), https://calawyers.org/privacy-law/ninth-circuit-holds-data-scraping-is-legal-in-hiq-v-linkedin/.

179. *Id.*

180. *Id.*

181. *Privacy Policy*, LINKEDIN, https://www.linkedin.com/legal/privacy-policy#use (Aug. 11, 2020).

data, such an outcome would have had disastrous anticompetitive effects on the industry.

B. *EPIC GAMES, INC. V. APPLE, INC.*

A more high-profile case, *Epic Games*, is another example where a Big Tech company asserted consumer privacy protections as a defense to alleged antitrust misconduct.[182] The triggering event for the lawsuit occurred when Epic Games updated its Fortnite app with a feature that allowed consumers to pay Epic directly, rather than paying through Apple's App Store.[183] This allowed Epic to bypass the App Store rules that required payments to go through the Apple payment system and Apple's thirty-percent commission fee.[184] In response, Apple pulled Fortnite from the App Store for violating App Store guidelines. That same day, Epic filed a lawsuit against Apple for removing the game.[185] Epic's lawsuit asserted that Apple's conduct violated federal and state antitrust laws, including California's UCL.[186] The U.S. District Court for the Northern District of California summarized Epic's claims as arguing that "Apple [was] an antitrust monopolist over (i) Apple's *own system* of distributing apps on Apple's *own devices* in the App Store and (ii) Apple's *own system* of collecting payments and commissions of purchases made on Apple's *own devices* in the App Store."[187] In sum, Epic argued that Apple illegally monopolized the iOS app distribution and in-app payments under the Federal Sherman Act and the California UCL.[188]

In response, Apple justified its control over the iOS app distribution and in-app payments in the name of consumer privacy and security.[189] Apple argued that its prohibition of third-party app stores ensures a "safe and secure ecosystem" that benefits both users, who enjoy stronger privacy protections, and Apple, which uses privacy and security to differentiate itself from its competitors.[190] Tim Cook, Apple's CEO, testified that privacy is a key factor for consumers who choose Apple.[191] Apple's internal surveys showed that privacy and security were important factors for fifty to sixty-two percent of users purchasing an iPhone.[192] Additional evidence also showed that Apple's

182. 559 F. Supp. 3d 898, 921–22 (N.D. Cal.), *appeal filed*, No. 21-16506 (9th Cir. Sept. 13, 2021), *granting stay*, No. 21-16506, 2021 WL 6755197 (9th Cir. Dec. 8, 2021).

183. Malcom Owen, *Epic Games v. Apple Trial, Verdict, and Aftermath – All You Need To Know*, APPLEINSIDER (Mar. 26, 2022), https://appleinsider.com/articles/20/08/23/apple-versus-epic-games-fortnite-app-store-saga----the-story-so-far.

184. *Id.*

185. *Id.*

186. *Epic Games*, 559 F. Supp. 3d at 921.

187. *Id.*

188. *Id.* at 921, 1033, 1051.

189. *Id.* at 922–23.

190. *Id.* at 1002.

191. *Id.* at 1007.

192. *Id.*

restrictions benefitted users who value their Apple products for their privacy and security features because the restrictions allowed them greater use of their devices.[193] The court found that witnesses were "unanimous that use security and privacy are valid procompetitive justifications"[194] and that "Apple's security rationale is a valid business justification for app distribution restrictions."[195]

After balancing the anticompetitive effects against Apple's justifications, the court held that Epic did not meet its burden of showing "that its proposed alternatives [we]re virtually as effective as the current distribution model" and found that Apple's conduct did not violate the Sherman Act.[196] However, the court did rule that Apple's anti-steering provisions, which limited developers from communicating with consumers about alternatives to Apple's in-app purchasing system,[197] violated the UCL.[198] The court reasoned that the harm from the anti-steering provisions outweighed the benefits because they gave Apple an unfair advantage and concealed information from consumer choice.[199] As such, Judge Yvonne Gonzalez Rogers issued an injunction prohibiting Apple from including external links or other actions that direct consumers to purchasing mechanisms from the developers' apps.[200] Judge Gonzalez Rogers also ruled that Apple may not prohibit developers from "communicating with customers through points of contact obtained voluntarily from customers through account registration within their app."[201] Judge Gonzalez Rogers did not make any rulings regarding privacy issues relating to Apple's anti-steering provisions, but found that Apple's security and privacy business justifications for app distribution restrictions defeated Epic's Sherman Act violation claims.[202]

There was no clear-cut winner in *Epic Games*. Apple was found not in violation of federal antitrust law, but was nevertheless required to eliminate its anti-steering provisions under the California UCL.[203] In response to Judge Gonzalez Rogers's decision, Apple released a statement that "success is not illegal," that the company "faces rigorous competition in every segment in which [it] do[es] business," and that it "believe[s] customers and developers choose [it] because [its] products and services are the best in the world."[204] Tim Sweeny, the CEO of Epic, also tweeted a statement saying: "Today's ruling isn't a win for developers or for consumers. Epic is fighting for fair competition among in-app payment methods and app stores for a billion consumers," and that "Fortnite

193. *Id.*
194. *Id.*
195. *Id.* at 1038.
196. *Id.* at 1041.
197. *Id.* at 1054–55.
198. *Id.* at 1057.
199. *Id.*
200. *Id.* at 1058.
201. *Id.*
202. *Id.* at 1038–39, 1058.
203. *Id.* at 1068.
204. Owen, *supra* note 183.

will return to the iOS App Store when and where Epic can offer in-app payment in fair competition with Apple in-app payment, passing along the savings to consumers."[205] Two days after the ruling, Epic filed its appeal to the Ninth Circuit.[206] Following the appeal, Sweeny again tweeted that Apple had told Epic that Fortnite would be blacklisted from the App Store until the resolution of the appeal.[207] Sweeny stated that this decision could keep Fortnite off Apple platforms for as long as five years.[208] The Fortnite app is still currently unavailable on the App Store.[209]

Although Apple was found to be in violation of the California UCL, *Epic Games* still exemplifies privacy's effectiveness as a shield against alleged antitrust misconduct. Unlike LinkedIn, Apple was able to successfully assert user privacy protection as a justification for alleged antitrust misconduct under the Sherman Act. The court accepted Apple's security and privacy concerns as a valid business justification for its app-distribution restrictions. Apple cited internal surveys and provided data on the importance of privacy for consumer choice. Apple is an industry leader in the smart-devices trade[210] and was able to leverage that in its defense. It continues to argue that its products are superior to its competitors' due not only to the quality of its products, but also the level of privacy and security it provides to consumers. According to Apple's Privacy Policy, Apple "retains personal data only for so long as necessary to fulfill the purposes for which it was collected."[211] Compared to other companies, such as Google, Facebook, Twitter, or Amazon, Apple offers some of the strongest privacy protections to its users because its business model isn't dependent on selling personal information.[212] Apple's clout in the technology industry, especially its renowned privacy protections, have allowed it to prevail thus far in an antitrust suit by asserting a privacy defense. Apple's reputation as a pro-privacy company provided it with a foundation for raising privacy and security concerns as a justification for its prohibition of third-party app stores, and making it difficult for Epic to rebut Apple's pro-privacy defenses.

205. Dustin Bailey, *Despite the End of Epic vs. Apple, Fortnite Isn't Coming Back to iOS Yet*, PCGAMESN (Sept. 10, 2021, 2:03 PM), https://www.pcgamesn.com/fortnite/ios-2021.

206. Owen, *supra* note 183.

207. Nicole Carpenter, *Fortnite 'Blacklisted' by Apple, Epic Games CEO Says*, POLYGON (Sept. 22, 2021, 1:19 PM), https://www.polygon.com/22688008/fortnite-blacklisted-epic-games-apple-store-ios.

208. *Id.*

209. *See App Store*, APPLE, https://www.apple.com/app-store/ (last visited Jan. 28, 2023).

210. *See generally* Kif Leswing, *Apple Claims Global Smartphone Market Lead Head of Samsung for First Time Since 2016*, CNBC, https://www.cnbc.com/2021/02/22/apple-beats-samsung-takes-global-smartphone-lead-in-q4.html (Feb. 22, 2021, 1:08 PM).

211. *Apple Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (Oct. 27, 2021).

212. Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, SECURITY.ORG, https://www.security.org/resources/data-tech-companies-have/ (July 22, 2022).

IV. PRIVACY AS A SWORD

As Big Tech antitrust defendants have begun using privacy defenses as a shield, plaintiffs have also begun raising privacy concerns as a sword in their complaints. Antitrust regulators have begun to view the degradation of privacy as a form of diminished quality that harms competition.[213] In a news conference, former U.S. Assistant Attorney General Makan Delrahim stated that "[p]rivacy can be an important dimension of quality. By protecting competition, we can have an impact on privacy and data protection. Moreover, two companies can compete to expand privacy protections for products or services, or for greater openness and free speech on platforms."[214] As such, privacy may become a significant factor in antitrust enforcement against Big Tech companies.

In the last couple of years, there have been multiple antitrust lawsuits in which private and government plaintiffs have asserted privacy concerns against Big Tech companies. This Part examines a number of these cases and analyzes the privacy concerns raised, along with the implications of such litigation.

A. *KLEIN V. FACEBOOK, INC.*

Recently in 2020, Facebook was struck with an antitrust class action complaint accusing it of monopolizing the social media and social network markets.[215] It is important to note that the plaintiffs recognized that consumers consented to giving up personal information and to receiving targeted advertisements on Facebook in exchange for free access to the platform.[216] Despite such consent to give up personal information, the plaintiffs alleged that Facebook had engaged in a "two-part anticompetitive scheme."[217] First, Facebook had allegedly "consistently and intentionally deceived consumers about the data privacy protections it provided to its users."[218] During the early age of social media, Facebook distinguished itself from competitors like MySpace by promising users stringent privacy protections.[219] The plaintiffs argued that as a result, many users chose Facebook over competing platforms.[220]

The complaint referenced numerous examples in which Facebook deceived its users about its privacy protections.[221] For example, in 2006, Facebook introduced the "News Feed" feature, which created a curated feed alerting users

213. Makan Delrahim, Assistant Att'y Gen., U.S. Dep't of Just., Remarks at the Antitrust New Frontiers Conference (June 11, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers.

214. *Id.*

215. Class Action Complaint at 71–78, Klein v. Facebook, Inc., 580 F. Supp. 3d 743 (N.D. Cal. Jan. 14, 2022) (No. 20-cv-08570).

216. *Id.* at 3.

217. *Id.* at 1.

218. *Id.*

219. *Id.*

220. *Id.*

221. *See id.* at 8–63.

of their friends' profile updates.[222] There was initial outcry from users arguing that the feature was too intrusive.[223] Facebook publicly reassured its users that it had enhanced privacy settings allowing users to keep their activities private, and that "industry-leading privacy restrictions . . . have made Facebook a trusted site for sharing information."[224] Despite this promise to provide users with enhanced privacy protection, Facebook made user content and information available to advertisers without disclosure or consent.[225] Another example cited was Facebook's Beacon Program, which allows third parties to track users' purchases on third-party websites and users to notify their Facebook friends of such purchases.[226] When launching the program, Facebook maintained that Beacon would only track and keep activity of users who consented through a permission-seeking pop-up.[227] However, Beacon allowed Facebook to track even the activity of users who clicked the "No, Thanks" prompt.[228] The plaintiffs alleged that Facebook's deception allowed it to gain illegal control over the social media and network market.[229]

Second, the complaint alleged that Facebook "exploited the rich data it deceptively extracted from its users to identify nascent competitors and then 'acquire, copy, or kill' these firms."[230] The plaintiffs argued that Facebook had used valuable consumer data to identify competitors without consumer consent.[231] Using the data, Facebook allegedly could copy competitors' innovations and force them to either sell at a bargain or face Facebook's "destroy" tactics to eradicate them from the market.[232] For example, in 2013, Facebook acquired Onavo, an Israeli mobile web analytics company, and used Onavo's data for surveillance.[233] Prior to Onavo's acquisition, Facebook had relied on Onavo's data to acquire Instagram.[234] The complaint alleged that "Facebook used Onavo's data to: (a) identify and target competitors from which Facebook could demand concessions; (b) identify and target competitors to whom Facebook would completely deny access to its platform; and (c) identify and target competitors that Facebook would remove from the competitive landscape entirely through acquisition."[235]

222. *Id.* at 31.
223. *Id.*
224. *Id.*
225. *Id.* at 31–32.
226. *Id.* at 32–33.
227. *Id.* at 33.
228. *Id.*
229. *Id.* at 1.
230. *Id.* at 2.
231. *Id.*
232. *Id.*
233. *Id.* at 44.
234. *Id.*
235. *Id.* at 45.

In January 2022, Judge Koh granted and denied in part Facebook's motion to dismiss in the U.S. District Court for the Northern District of California.[236] Judge Koh allowed the consumer class action to carry on with allegations that Facebook unlawfully used consumer data to stifle competition, determining that the plaintiffs alleged with "sufficient particularity that Facebook made numerous 'clearly false' representations about its collection and monetization of data."[237] Judge Koh acknowledged consumers' allegations that Facebook's systematic deception about user data allowed it to beat out competitors who were truthful about their data practices or did not collect or sell user data.[238] However, Judge Koh threw out the claims regarding Facebook's "copy, acquire, kill" tactics as untimely.[239] The plaintiffs had failed to assert any overt acts of Facebook's "copy, acquire, kill" strategy that occurred after December 3, 2016, or four years before filing the lawsuit.[240]

Judge Koh also denied Facebook's motion to dismiss the plaintiffs' Sherman Act claim, which alleged that Facebook acquired and maintained monopoly by making false representations to users about its data privacy practices, determining that they sufficiently stated a claim for "false and misleading advertising."[241] The court cited a Ninth Circuit decision that held that a company's false and misleading advertising may amount to exclusionary conduct for the purposes of the Sherman Act.[242] To bring a Sherman Act claim based on false and misleading advertising,

> a plaintiff must show that the company made representations about its own products or its rivals' products that "were [1] clearly false, [2] clearly material, [3] clearly likely to induce reasonable reliance, [4] made to buyers without knowledge of the subject matter, [5] continued for prolonged periods, and [6] not readily susceptible of neutralization or other offset by rivals."[243]

After assessing the plaintiffs' allegations, the court ruled that they had adequately pleaded that Facebook's false representation about its data privacy practices qualified as exclusionary conduct under the Sherman Act.[244] The court also ruled that the consumers had adequately pleaded causal antitrust injury by asserting that Facebook's monopolization of social media and social network markets harmed users because it allowed the company to "extract additional 'personal information and attention' from users."[245] The complaint set forth in detail that "personal information and attention" has significant material value

236. Klein v. Facebook, Inc., 580 F. Supp. 3d 743, 759 (N.D. Cal. 2022); *see also supra* note 31.
237. *Id.* at 795.
238. *Id.* at 793.
239. *Id.* at 819.
240. *Id.*
241. *Id.* at 804–05.
242. *Id.* at 785.
243. *Id.*
244. *Id.* at 802.
245. *Id.*

because Facebook sells user data to third parties, including advertisers, and monetizes user information through targeted advertisements.[246] Accordingly, the court ruled that the plaintiffs could carry on with their data privacy claims under the Sherman Act.

Klein v. Facebook, Inc. is an early example of plaintiffs successfully asserting data protection privacy concerns in an antitrust complaint. The case is still in its early stages, and the court has yet to weigh the merits of the plaintiffs' claims. However, Judge Koh's decision to allow consumers to proceed with these allegations may set a precedent for future antitrust and data privacy consumer class actions. This type of argument may become common in antitrust cases in which the defendant does not charge its users for access to its platform but sells users' data for profit.

B. *UNITED STATES V. GOOGLE LLC*

In October 2020, the DOJ and several states filed an antitrust enforcement action against Google for "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."[247] The complaint incorporates privacy concerns in its allegations of Google's anticompetitive effects "foreclos[ing] competition for internet search."[248] For years, Google has entered into exclusionary agreements and engaged in anticompetitive conduct "to lock up distribution channels and block rivals."[249] The complaint cites the fact Google paid *billions* of dollars each year to distributors such as Apple, LG, Motorola, Verizon, and AT&T to secure Google as the default preinstalled search engine and prohibit counterparties from dealing with Google's competitors.[250]

Importantly, the complaint alleges that Google's anticompetitive 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 in general services, and impeding innovation."[251] For example, DuckDuckGo, a search engine platform that differentiates itself from Google by its protective privacy policies, has largely been denied from entering the search engine market.[252] The complaint alleges that "Google's control of search access points means that these new search models are denied the tools to become true rivals: effective paths to market and access, at scale, to consumers, advertisers, or data."[253] Due to Google's anticompetitive conduct, American

246. *Id.*
247. Complaint at 2, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020).
248. *Id.* at 4.
249. *Id.* at 3–4.
250. *Id.*
251. *Id.* at 53.
252. *Id.* at 5.
253. *Id.*

consumers are allegedly forced to accept Google's privacy practices and use of personal data as new companies are unable to compete against Google's "long shadow."[254] As of January 2023, the case is still pending,[255] and the parties are undergoing an extensive discovery battle, with the DOJ alleging that Google committed privilege abuse.[256]

The case is yet another example of plaintiffs asserting privacy complaints in an antitrust lawsuit involving a defendant that does not charge its users a fee to access its platform. Although the case is still pending and the court has yet to weigh the merits of the claims, this case may also become a precedent for government plaintiffs asserting privacy concerns in antitrust enforcement actions. The eventual resolutions in both *Klein* and *Google* could significantly alter the legal landscape for cases that involve the intersection of data privacy and antitrust.

V. CONSEQUENCES OF USING DATA PRIVACY AS A SHIELD AND SWORD IN ANTITRUST VIOLATIONS FOR REGULATORY, LITIGATION, AND CORPORATE PRACTICES

Privacy is increasingly becoming a significant factor in antitrust litigation, both as justification to defend against alleged anticompetitive conduct and as an element of product quality that can be diminished as a consequence of alleged anticompetitive conduct.[257] This trend will continue in litigation and will in turn affect the legal landscape, along with corporate practice. Given the recent antitrust litigation involving both defendants and plaintiffs raising privacy concerns, this Part examines the consequences of using data privacy as a shield and sword to alleged antitrust misconduct from a regulatory, litigation, and corporate perspective.

The trend of incorporating privacy into antitrust litigation will continue. In the last year, the Biden Administration made three key appointments that could potentially impact the future of antitrust and privacy.[258] First, President Biden nominated Lina Khan, who was confirmed by the Senate to serve as the Chair of the FTC.[259] Khan, a strong proponent of the Hipster Antitrust movement, has published literature discussing the implications of Big Tech companies handling vast amounts of user data.[260] In a 2019 *Harvard Law Review* article discussing the relationship between privacy and antitrust, Khan and her coauthor wrote that "any broad regulatory framework . . . that focuses on abusive data practices[]

254. *Id.* at 7.

255. *U.S. and Plaintiff States v. Google LLC*, U.S. DEP'T OF JUST., https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc (Sept. 28, 2022).

256. Dave Simpson, *DOJ Says Google's 8,000 New Releases Show Privilege Abuse*, LAW360 (Apr. 7, 2022, 7:24 PM), https://www.law360.com/articles/1481946/doj-says-google-s-8-000-new-releases-show-privilege-abuse.

257. Scarborough et al., *supra* note 22.

258. *Id.*

259. *Id.*

260. *Id.*

without attending to issues of market structure is likely to be at best highly incomplete and at worst an impediment to necessary reforms."[261] Thus, Khan's appointment may lead to more robust antitrust enforcement that incorporates data privacy in its review.

President Biden also nominated Alvaro Bedoya, who was confirmed by the Senate to serve as an FTC Commissioner.[262] Bodeyo founded Georgetown's Center on Privacy & Technology and has written extensively on privacy-related topics and issues,[263] and will bring a fresh privacy perspective to the FTC. Finally, President Biden appointed Tim Wu to serve as Special Assistant to the President for Technology and Competition Policy.[264] Wu, the author of *The Curse of Bigness: Antitrust in the New Gilded Age*, has criticized tech firms for their anticompetitive conduct, which he argues allows them to get away with deficient data privacy protections.[265] Wu may bring this perspective into his role. Given President Biden's pro-privacy nominations to his Administration, it is likely that regulators will wield privacy concerns in antitrust enforcement.

Additionally, in July 2021, President Biden issued Executive Order 14036, Promoting Competition in the American Economy, focused specifically on the technology industry.[266] It states:

> [I]t is the policy of [the] Administration to enforce the antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially as they stem from serial mergers, the acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects.[267]

As for the judicial landscape, it is likely that more courts will accept privacy claims and defenses in antitrust litigation, especially in light of *hiQ Labs* and *Klein*. It is also likely, depending on the outcomes of *Klein* and *Google*, that more consumer class actions against Big Tech companies will be brought. Both cases involve antitrust defendants who rely on selling consumer data for profit and have faced the most scrutiny regarding their lack of data privacy protections.

The law has only barely begun to scratch the surface in addressing the intersection between antitrust and data privacy. Courts are also likely to consider both in conjunction, given the current Administration and its scrutiny of Big Tech. However, legislators and regulators must work together to intertwine the bodies of data privacy and antitrust law to create a more robust analysis of data privacy in antitrust litigation.

---

261. *Id.*
262. *Id.*
263. *Id.*
264. *Id.*
265. *Id.*
266. Exec. Order No. 14036, 86 Fed. Reg. 36987 (July 9, 2021).
267. *Id.* at 36988.

Big Tech companies are no strangers to antitrust litigation or regulatory penalties. When the political consultancy Cambridge Analytical improperly obtained the data of about eighty-seven million Facebook users, Facebook was fined $5 billion.[268] In the wake of the scandal, Mark Zuckerberg, Facebook's CEO, made several promises such as creating a "clear history" tool to delete all data Facebook gathers about users as they browse the web and creating an end-to-end encryption for all of Facebook's messaging platforms.[269] Despite the record-breaking fine that Facebook was forced to pay, Facebook has yet to fulfill its promises on its privacy policy reforms.[270]

Tech companies whose business models rely on collecting and selling data seem unlikely to change their corporate privacy policies as a result of litigation.[271] Companies like Facebook continue to announce empty promises regarding their privacy practices with no actual intent to change their business models. Although the integration of privacy is becoming prevalent in antitrust litigation, it is unlikely that data-business tech companies will change their corporate privacy practices without legislation or government enforcement. By contrast, Apple, whose business model does not solely rely on collecting and selling data, has actually created more robust privacy practices in light of recent data privacy scandals.[272] In April 2021, Apple released a new iOS update that allows users to opt out of tracking on third-party apps that monitor users' behavior and share that data with third parties.[273] This feature has caused backlash from tech companies, including Facebook and Google, that heavily rely on such data to support their business models.[274] In sum, companies whose profit models heavily depend on the sale of user data are unlikely to change their corporate practices even in light of countless consumer class-action suits or lawsuits over clearly problematic data privacy practices, because doing so would not be profitable.

Privacy experts need a seat at the antitrust table. For antitrust agencies to address data-driven competition, they must work with data protection regulators. The collection and usage of personal data by data-driven companies like Facebook and Google has granted them extraordinary monopolistic powers. Data privacy regulators alone are not equipped to deal with such data collection

268. *Facebook 'To Be Fined $5bn over Cambridge Analytica Scandal,'* BBC NEWS (July 13, 2019), https://www.bbc.com/news/world-us-canada-48972327.

269. Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World - but It Didn't Change Facebook*, THE GUARDIAN (Mar. 18, 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

270. *Id.*

271. *Id.*

272. Laurel Wamsley, *Apple Rolls Out Major New Privacy Protections for iPhones and iPads*, NPR (Apr. 26, 2021, 4:12 PM), https://www.npr.org/2021/04/26/990943261/apple-rolls-out-major-new-privacy-protections-for-iphones-and-ipads.

273. Rebecca Heilweil, *Why the New iOS Update Is Such a Big Deal*, VOX (Apr. 26, 2021, 10:52 AM), https://www.vox.com/recode/22393931/facebook-ios-14-5-app-tracking-transparency-iphone-privacy.

274. *Id.*

and use. Antitrust agencies must make an effort to integrate both privacy and antitrust review to ensure that data-driven tech behemoths are not committing anticompetitive conduct while misusing consumer data. Data protection agencies in the European Union and United Kingdom have started to work with antitrust agencies.[275] The United States must follow in the same footsteps. President Biden's new leadership at the FTC and his recent executive order on competition appear to favor integrating privacy into antitrust review.

CONCLUSION

The synthesis of antitrust and data privacy is inevitable. Recent litigation trends show that it is becoming increasingly acceptable to use data privacy as a business justification for alleged antitrust misconduct, and conversely, to raise data privacy concerns against antitrust defendants. The current antitrust and privacy legal landscape has yet to account for the integration of both areas of law. However, it is crucial for privacy experts to work with antitrust regulators to furnish robust antitrust enforcement against Big Tech companies. Given the likelihood that data privacy and antitrust litigation will continue to increase, a collaboration between privacy and antitrust experts will allow for a better understanding of the scope of privacy in antitrust enforcement.

Consumers and technology companies must closely watch the Biden Administration's FTC management, especially in light of the President's pro-privacy appointments. It is likely that current regulators will advocate for the inclusion of privacy in antitrust enforcement, which may ultimately affect litigation in this space. However, it seems unlikely that such litigation or regulation will affect Big Tech companies' corporate privacy practices, especially those whose business models are dependent on selling user data. Regardless, the integration of antitrust and data privacy is rising to prominence, and their inevitable intersection must be reconciled in both litigation and regulation.

275. Jami Vibbert, John Schmidt & Debbie Feinstein, *Trend To Watch: Antitrust and Data Protection Regulators Seek Greater Alignment in 2022—Big Data May Be a Target*, ARNOLD & PORTER (Jan. 31, 2022), https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2022/01/data-protection-regulators-seek-greater-alignment.