What is Privacy—to Antitrust Law

Erika M. Douglas*

From President Biden to the Chair of the Federal Trade Commission, there is dramatic new attention to the overlap between data privacy and competition. Our personal data now fuels the online world, from search and social media to applications and algorithms. While privacy law limits the processing of such data, antitrust law often encourages it to drive online competition. This is creating new interactions—and tensions—between these powerful areas of law.

This Article argues that antitrust law has been too singular in its treatment of data privacy. Antitrust scholars, courts, and agencies cast data privacy the same way across this variety of new interactions: as a quality-like factor that rises and falls with competition. Yet privacy is notoriously pluralistic in its identity. No single definition of data privacy has coalesced in the law, nor is a unitary conception likely to emerge. The Article contends that the cramped antitrust view of data privacy is a significant problem. It leads courts and lawmakers to unexamined preferences for competition over data privacy, which can threaten the already-fragile recognition of harms within privacy law itself.

In particular, the Article explores two seismic shifts underway in U.S. data privacy law—i) the move away from notice and consent toward more prohibitions and duties, and ii) the proliferation of privacy rights. These changes erode the basis on which antitrust reconciles data privacy: a previously-shared assumption that consumers benefit from personal data-driven competition. As a result, these shifts are creating new variety and complexity in how antitrust and privacy law interact.

It argues these changes will press antitrust to develop more pluralistic thinking of what privacy is to antitrust law. The Article proposes a number of important ways in which antitrust can begin to do this, both institutionally and substantively. In particular, it draws analogies to antitrust theory on other incommensurate interests, such as patent rights, free speech rights, and regulation, that, like privacy, can require theories of exception and conflict where they meet antitrust law.

---

* Associate Professor of Law, Temple University Beasley School of Law. Thank you to Peter Swire, Kirsten Martin, John M. Yun, Christopher Leslie, the participants of the 2022 Privacy Law Scholars Conference, and the Competition, Antitrust Law & Innovation Forum Roundtable at the University of California, Irvine School of Law for their thoughtful comments on earlier versions of this draft.

INTRODUCTION

From the President himself[1] to the Chair of the Federal Trade Commission,[2] there is dramatic new attention to "the overlap between data privacy and competition."[3] This overlap is clearest where our personal data fuels competition. A myriad of companies use our data to offer digital services, from social media and online search to applications and algorithms. That data is used to make decisions about our credit, education, health and more. Antitrust law seeks to promote competition among these services, which often means encouraging *more* access to our personal data. Meanwhile, data privacy law seeks to protect our interests in that same data, which often means encouraging *less* access to it.[4]

Data privacy has begun to appear across antitrust law, from theories of liability and defenses to remedies, legislation, and policy. In high-profile antitrust cases, U.S. enforcers claim that digital giants Google and Facebook used their market power to erode online data privacy.[5] At the same time, other large technology companies invoke user privacy protection as a defense to antitrust claims. In the Ninth Circuit, Apple argued successfully that it blocked competitors from its online app store to better compete based on privacy protection for end users—rather than to

---

1. Promoting Competition in the American Economy, 86 Fed. Reg. 36987 (July 14, 2021) (executive order on *Promoting Competition in the American Economy* requiring heads of federal agencies to consider using their authority to "facilitate innovation that fosters United States market leadership and market entry to *promote competition* and economic opportunity and to resist monopolization, while also ensuring safety, *providing security and privacy* . . . .") (emphasis added).

2. The Federal Trade Commission is one of two federal agencies that enforce antitrust law in the United States, along with the Department of Justice Antitrust Division.

3. FED. TRADE COMM'N., FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 4 (Sept. 13, 2021), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf [https://perma.cc/NAK9-VYKR] (emphasizing that the agency will "spend more time on the overlap between data privacy and competition"); *See also Nominations Hearing: Questions for the Record Jonathan Kanter Nominee to be Assistant Attorney General of the Antitrust Division Before the S. Comm. on the Judiciary*, 117th Cong. 2 (2021) (showing responses of Jonathan Kanter to questions from Sen. Chuck Grassley, Ranking Member, S. Comm. on the Judiciary) ("Effective antitrust enforcement should address the full range of competitive harm in markets involving the extraction and use of data. These include, among other things, *harms related to privacy*, innovation, resiliency of technology infrastructure.") (emphasis added).

4. This Article uses the term "data privacy law" to denote the laws that govern the collection, processing, and transfer of our personal information. While the concepts are distinct, this is analogous to the term "data protection" law used in the European legal context. *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 775 (2019) ("'Data protection' is the accepted, standard term applied to Europe's body of law concerning the processing, collection, and transfer of personal data."). Both concepts are narrower than, and often distinguished from, the broader body of "privacy law," which encompasses decisional, spatial, and other types of privacy. These concepts may relate to personal data but are less focused on the data itself.

5. Substitute Amended Complaint for Injunctive and Other Equitable Relief, F.T.C. v. Meta Platforms, Inc. (previously known as Facebook), No. 20-cv-03590 (D.D.C. Sept. 8, 2021); Complaint, United States et al. v. Google, LLC, No. 20-CV-03010 (D.D.C. Oct. 20, 2020); *See also* Press Release, Bundeskartellamt v. Facebook, B6-22/16 (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html [https://perma.cc/U3NG-DYM9] (Ger.).

monopolize app distribution on iPhones, as the plaintiff claimed.[6] Proposed antitrust legislation seeks to require dominant digital platforms like Amazon and Apple to interoperate with rivals, in an effort to restore online competition.[7] Since this interoperability would increase access to personal data on such platforms, the legislation includes exceptions meant to protect our privacy.[8]

Across this variety of interactions, antitrust theory tends to treat data privacy as one thing—a parameter of quality in products or services.[9] Antitrust posits that online services compete to offer a greater level of privacy to end users.[10] For example, online internet browsers might compete to win customers by offering more privacy-protective settings, settings that allow those customers to opt out of the collection or sale of personal data. This competition between internet browsers would be expected to increase the quality of privacy protection offered in the market, as each company tries to attract users with more privacy-protective settings.

But, if there is one thing antitrust should know about privacy, it is that privacy is *not* one thing. Privacy scholarship has long been fond of asking, "What is privacy?," inspiring the title of this Article.[11] The answers are famously variable.[12] Privacy scholars trace the roots of privacy to conceptions of control, solitude, confidentiality, freedom, autonomy, intimacy, dignity, and more.[13] Nor does privacy

---

6. *See* Epic Games, Inc. v. Apple, Inc., 67 F.4th 946, 985–86 (9th Cir. 2023) (affirming the District Court finding that Apple established a justification for its conduct based on privacy competition); *See also* hiQ Labs, Inc. v. LinkedIn, Corp., 31 F.4th 1180 (9th Cir. 2022) (LinkedIn claiming data privacy protection as a justification in response to allegations of state antitrust law violations), *order dissolved* on unrelated grounds No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022).

7. *See, e.g.*, American Choice and Innovation Online Act, H.R. 3816, 117th Cong. (2021-2022) (seeking to improve digital competition by prohibiting covered platforms from materially restricting interoperability with rivals); American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021–2022) (same); Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, H.R. 3849, 117th Cong. (2021–2022) (mandating interoperability with large social media services to promote competition); Open App Markets Act, S. 2710, 117th Cong. (2021–2022) (requiring that covered companies allow interoperability with competing apps and app stores).

8. *See, e.g.*, American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(b)(I) (2021–2022).

9. *See infra* Part I. B. The Current Theory: Antitrust Understands Privacy as an Element of Product or Service Quality.

10. *Id.*

11. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (Harvard Univ. Press ed., 2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY].

12. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482–83 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] (tracing the history of "various [scholarly] attempts at explicating the meaning of 'privacy'" from 1980 to present and offering a new taxonomy of privacy harms); Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski & Masa Galic, *A Typology of Privacy*, 483 U. PA. J. INT'L L. 483, 487–88 (2017) (observing that "[p]rivacy is notoriously hard to capture" and describing an array of scholarly efforts to define "what privacy means").

13. Solove, *A Taxonomy of Privacy*, *supra* note 12, at 479–80 (noting repeated observations from scholars on the difficulty in defining privacy and that the concept "suffers from an embarrassment of meanings"); Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1677 (2021) ("Throughout history, privacy has evaded a precise meaning."); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 406 (2015) ("Privacy theorists differ

have a single identity in the law. In 1890, Samuel Warren and Louis Brandeis framed the earliest conceptions of privacy in tort.[14] Since then, the term "privacy law" has grown to span the 1L curriculum, with facets of constitutional,[15] contract,[16] consumer protection,[17] and even property law.[18] After much examination, influential recent scholarship casts privacy as "an umbrella term" that unites a variety of concepts.[19] In short, privacy is pluralistic.[20] This diversity of privacy identities is nowhere to be found in the antitrust treatment of data privacy.

This Article considers the specific question of what privacy is to antitrust law. It argues that existing antitrust theory on data privacy is too unitary, and fails to capture the pluralistic nature of new interactions between antitrust and privacy law.

Part I introduces the prevailing antitrust theory of data privacy in judicial, agency, and scholarly dialogues. This theory treats data privacy as an element of product quality. It makes for a tidy reconciliation between privacy and antitrust law, premised on the shared assumption that consumers benefit from making privacy choices in markets for personal data.

Part II argues that this cramped antitrust view of data privacy is problematic. This view is leading to unexamined preferences for competition over data privacy in judicial decisions, legislation, and agency perspectives. Weak antitrust conceptions of privacy can even pose a risk to standalone privacy law, through the shared development of the common law.

Part III examines two paradigm shifts underway in U.S. data privacy law—the move away from notice and consent-based privacy protection toward prohibitions and duties, and the proliferation of privacy rights. It argues that these developments are fragmenting the landscape of privacy and antitrust interactions, because they erode the previously shared assumption that the commercialization of personal data is positive for consumers. As a result, the Article argues that both changes will press

---

famously and widely on the proper conception of privacy.").

14. Warren & Brandeis, *supra* note 11, at 195 (conceiving of the "the right to be let alone" in tort); *see also* Prosser, *supra* note 11 (describing privacy torts).

15. *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967); United States v. Jones, 565 U.S. 400, 405-408 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

16. Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91–92 (1999) (finding privacy policies enforceable as contracts). *But see* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–96 (2014) (observing that, despite early indications otherwise, contract law now plays a relatively minimal role in privacy protection).

17. *See, e.g.*, 15 U.S.C. § 45(a)(1) (2018).

18. Lawrence Lessig, *Privacy as Property*, 69 SOC. RES.: AN INT'L Q. 247 (2002) (arguing that "property talk" would strengthen the rhetorical force behind privacy).

19. Hartzog, *supra* note 13, at 1680; SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 40 ("[P]rivacy is not one thing, but a cluster of many distinct yet related things."); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67 (9th ed. 2010) ("One point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject.").

20. Koops et al., *supra* note 12, at 487 (noting numerous scholars "offer typological or pluralist conceptions of privacy").

antitrust to develop more pluralistic theories of data privacy. Antitrust analysis can no longer presume that data privacy is relevant only to the extent it is subsumed into analysis of competitive effects.

Finally, Part IV looks ahead to consider how antitrust can develop conceptions of what privacy is that better reflect the reality of privacy law itself. First, it calls for antitrust institutions of all types to build greater "privacy competency"—a willingness and ability to delve into and understand the privacy interests and rights protected by the new world of privacy law— and considers how to achieve this in practical terms. Second, it explores how legislatures and courts can develop their thinking about tensions, exceptions, and conflicts where competition and privacy collide. It develops this understanding by analogy to antitrust theory where it interacts with other incommensurate interests, such as patent rights, free speech rights, and industry regulation. Like privacy, these interests can, at times, be countervailing and difficult to reconcile with the competition sought by antitrust law, but each offers rich theories that inform the reconciliation of privacy and antitrust.

The Article offers several contributions to the literature. It is the first to challenge the accepted theory on antitrust and data privacy as too singular. This criticism develops the socio-legal importance of data privacy harms, which are often underrecognized in the law. It does so by identifying a previously-unacknowledged preference for competition over privacy appearing in judicial decisions, proposed legislation, and agency perspectives. Then, it offers the first examination of how antitrust law could treat data privacy as a serious and distinct area of legal doctrine. This contributes to the legal recognition of privacy harms by resisting their assumed subsidiarity where privacy interests are in tension with competition.

More broadly, the Article contributes to a shared dialogue between antitrust experts and privacy experts. Both antitrust and privacy law play powerful—and not always compatible—roles in the control of digital giants. Despite their mutual relevance to the digital economy, antitrust and privacy law exist in surprisingly separate worlds. This disconnect is a serious barrier to comprehensive digital regulation, as it leaves scholars, agencies, and lawmakers in each discipline talking past each other. In particular, the U.S. lags in its collaboration across these areas of law relative to other jurisdictions, which have already begun to conduct the first joint investigations,[21] and other cooperative action,[22] between the (often separate) agencies that enforce antitrust

---

21. U.K. INFORMATION COMMISSIONER'S OFFICE & U.K. COMPETITION MARKETS AUTHORITY, COMPETITION AND DATA PROTECTION IN DIGITAL MARKETS: A JOINT STATEMENT BETWEEN THE CMA AND THE ICO, 2021, at 29 (detailing the joint investigation of U.K. privacy authority and U.K. competition authority into Google's proposed termination of third-party cookies access to the Chrome internet browser). For an in-depth discussion of global developments at this interface of privacy and competition, see ERIKA DOUGLAS, DIGITAL CROSSROADS: THE INTERSECTION OF COMPETITION LAW AND DATA PRIVACY (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737 [https://perma.cc/8AXC-ADHJ].

22. *Big Data & Digital Clearinghouse*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en [https://perma.cc/N6NT-GFWV] (last visited Apr. 11, 2024) (detailing the European Digital Clearinghouse, established in

law and data privacy law. This Article promotes a more nuanced understanding across U.S. privacy and antitrust law that has become essential to effective digital regulation.

I. EXISTING ANTITRUST THEORY: A UNITARY PERSPECTIVE ON DATA PRIVACY

This Part examines the fairly short history of antitrust theories on data privacy. It introduces the prevailing theory of "privacy-as-quality," which—as the name suggests—treats privacy as an element of product quality. It then examines the shared assumption that underlies this antitrust theory and, at least until recently, data privacy law: that the commercial use of personal data is positive for individuals.

A. Early Theory on Antitrust and Privacy Emphasized Doctrinal Separation

The earliest theories on the interaction between antitrust and privacy emerged in the mid-2000s. Initial thinking emphasized the historical and doctrinal distinctions that separated the two areas of law. The Federal Trade Commission (FTC), which is the main U.S. federal privacy law enforcer, was initially created as a competition agency.[23] It was only later that Congress granted the FTC its separate consumer protection authority, amending Section 5 of the Federal Trade Commission Act through the passage of the Wheeler-Lea Act.[24] The new Section 5 empowered the agency to protect consumers from commercial harms by combatting misleading and deceptive business practices.[25]

Beginning in the mid-1990s, the FTC used this Section 5 consumer protection authority as a tool to protect data privacy. The FTC has used its power to prevent unfair or deceptive practices to uphold companies' privacy policies[26] and privacy settings[27] when companies seek to violate them. Section 5 has also been used to combat retroactive changes to those policies,[28] to prevent data collection using spyware[29] or unfair default privacy settings,[30] and to require adequate data privacy security practices.[31] Over time, this privacy enforcement under Section 5 has created

---

2017, is a platform to facilitate cooperation, dialogue, and information sharing between competition, consumer protection, and privacy regulators).

23. *See* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 138 n.78 (2015).

24. 15 U.S.C. § 45(a)(1) (2018) (providing the FTC with consumer protection powers).

25. *Id.*

26. *See, e.g.*, Complaint, Eli Lilly & Co., 133 F.T.C. 763 (2002) (alleging Eli Lilly company disclosed customers' personal information in violation of privacy policy).

27. Complaint at 4, Google Inc., FTC File No. 102 3136, No. C-4336 (F.T.C. Oct. 13, 2011) (alleging Google failed to observe privacy settings of users as part of the deceptive acts).

28. Decision and Order at 443, 446, Gateway Learning Corp., 138 F.T.C. 443 (2004) (alleging Gateway retroactively changed its privacy policy to permit personal data to be rented to third parties).

29. Aspen Way Enter., Inc., FTC File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013).

30. Complaint for Permanent Injunction and Other Equitable Relief at 19, FTC v. Frostwire, LLC, No. 11-cv-23643 (S.D. Fla. Oct. 12, 2011) (alleging Frostwire failed to notify users that, by default, previously downloaded files on users' computers were shared publicly even from "unshared" folders).

31. For an assortment of other practices that have been challenged under Section 5, see summary in Solove & Hartzog, *supra* note 16, at 627–43.

a body of FTC complaints and settlements, along with a few litigated cases, that together have been dubbed the U.S. "common law of [data] privacy."[32]

Early scholarly writing on antitrust and data privacy emphasized the need for continued separation between these two areas of FTC authority in competition and consumer protection law.[33] It argued that antitrust law was best suited to prevent conduct harmful to overall consumer welfare or economic efficiency in the marketplace.[34] Data privacy law, conceived of as a form of consumer protection law under Section 5, was better suited to ensure that individual consumers received the benefit of their bargains, because of its focus on informed choice and reasonable consumer expectations.[35]

This perspective was largely a response to concern that antitrust law would be distorted into an ill-fitting tool used to protect data privacy. In 2007, consumer privacy advocates were pressing the FTC to impose remedies on Google's acquisition of the ad-serving company DoubleClick.[36] The advocates worried that, post-transaction, the merging parties would combine their online advertising-related data sets, giving Google unprecedented access to user information and negatively impacting consumer privacy.[37] The FTC reviewed the merger under its Clayton Act authority, a part of antitrust law that empowers the agency to block mergers that substantially lessen competition.[38]

During the agency's review of this transaction, just one dissenting FTC Commissioner shared these privacy concerns and endorsed the idea that antitrust could be used to police privacy harms in mergers.[39] The FTC majority, however, rejected this view and refused to intervene in the Google/DoubleClick merger on privacy grounds.[40] The FTC majority saw any privacy effects as beyond the agency's authority to review the competitive effects of mergers. The majority explained that, although privacy protection was an important policy goal, the purpose of federal antitrust review of mergers is only to identify and remedy transactions that harm

---

32. *Id.* at 583 (describing and labelling the emergence of the FTC's "new common law of privacy," consisting of the common-law-like body of settlement agreements reached between the FTC and companies accused of unfair and deceptive trade practices).

33. *See* Ohlhausen & Okuliar, *supra* note 23, at 138–43.

34. *Id.* at 154–55.

35. *Id.*

36. *See* Statement of Federal Trade Commission Concerning Google/DoubleClick at 2–3, FTC File No. 071-0170 (F.T.C. Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [https://perma.cc/VBV6-MQ4S] (noting limits of FTC jurisdiction in declining to consider privacy when unrelated to quality-based competition) [hereinafter FTC Statement on Google/Doubleclick].

37. *Id.* at 2.

38. *Id.*

39. Dissenting Statement of Comm'r Pamela Jones Harbour at 10, Google/Doubleclick, Fed. Trade Comm'n. File No. 071-0170 (Dec. 20, 2007) (expressing greater concern over the privacy impacts of the transaction and considering "various theories that might make privacy 'cognizable' under the antitrust laws").

40. FTC Statement on Google/Doubleclick, *supra* note 36, at 2 (noting limits of FTC jurisdiction in declining to consider privacy when unrelated to quality-based competition).

competition.[41] There was no evidence of such harm to competition at the time of the Google/DoubleClick transaction.

Still, the perceived threat to antitrust doctrine had been established—antitrust law might be stretched to protect privacy. This push to extend antitrust law reappeared in objections to several subsequent mergers, including Google's acquisition of smart-device company Nest and Facebook's (now Meta) acquisition of online messaging company WhatsApp. This struck fear in the hearts of antitrust traditionalists, who worried that doctrinal confusion would be introduced by the application of antitrust law to privacy problems. This produced a dialogue dominated by theories that insisted on separation between antitrust and privacy law.[42]

This early theory of separation proved incomplete in the face of the growing digital economy.[43] It failed to account for the new and obvious privacy/competition interactions proliferating in policy and litigation. Privacy was appearing in various forms across antitrust claims, defenses, and remedies.[44] The insistence on separation between antitrust and privacy law offered no answers to important questions in these contexts: Were companies competing with each other to offer better privacy features in certain markets? Was monopoly power being used to erode digital privacy protection? Could the protection of data privacy constitute a justification for anticompetitive conduct in antitrust law?

B. The Current Theory: Antitrust Understands Privacy as an Element of Product or Service Quality

Over the last five years, the problems of online competition and online privacy have come to be viewed as intertwined.[45] Digital policy discussions now regularly mention privacy and competition in the same breath. President Joseph Biden's 2021 *Executive Order on Promoting Competition in the American Economy* emphasized the promotion of competition, but only while also ensuring privacy.[46] In a 2021 report to Congress, the FTC Chairwoman emphasized that "we need to make sure we are looking with both privacy and competition lenses at problems that arise in digital

---

41. *Id.*

42. *See* Ohlhausen & Okuliar, *supra* note 23, at 138 ("[S]uch commingling of the competition and consumer protection laws under any of these approaches is unnecessary and could lead to confusion and doctrinal issues in antitrust."); Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979) ("Congress designed the Sherman Act as a 'consumer welfare prescription.'") (quoting ROBERT BORK, THE ANTITRUST PARADOX 66 (1978)).

43. Erika Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J.F. 647, 658 (2021) (describing inadequacy of separatist theory).

44. See examples of these interactions at *supra* text accompanying footnotes 5–7.

45. Bennett Cyphers & Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, ELEC. FRONTIER FOUND. (Feb. 21, 2022), https://www.eff.org/wp/interoperability-and-privacy#Risksandmitigations [https://perma.cc/N7VF-T9GV]; Douglas, *supra* note 43.

46. Promoting Competition in the American Economy, Exec. Order No. 14036, 86 Fed. Reg. 36987, 36996 (requiring heads of federal agencies to consider using their authority to "facilitate innovation that fosters United States market leadership and market entry to promote competition and economic opportunity and to resist monopolization, while also ensuring safety, providing security and privacy . . . .").

markets."[47] This is in stark contrast to the earlier insistence on separation between the law of privacy and antitrust described above. It reflects a more realistic view of the interconnectedness of these areas of law and policy in the digital world.

As antitrust works to understand the relevance of data privacy, a new theory has taken hold among agencies, scholars, and policymakers to explain this legal interface. The U.S. antitrust enforcers—the FTC[48] and the Department of Justice, Antitrust Division (DOJ)[49]—as well as European competition authorities[50] have all begun to theorize privacy as an element of quality-based competition.

The theory is that, in certain markets, firms will compete to offer consumers better privacy protection, much like they would compete on other factors related to quality, such as new features or durability. This theory starts from the well-established position that consumer economic welfare is improved by competition based not only on price but also on other factors like quality.[51] It then interprets "quality" broadly to incorporate privacy as a parameter of quality-based competition in antitrust analysis.

Antitrust enforcers first began applying this "privacy-as-quality" theory in merger cases, and more recently it has appeared in anti-monopolization cases. For example, European competition authorities found privacy-quality effects were likely in their review of Microsoft's acquisition of LinkedIn.[52] The authorities concluded that Microsoft would integrate LinkedIn into its other services, such as the popular Windows operating system.[53] Microsoft was then likely to foreclose competition from more privacy-protective social networking services in the market, preventing those services from having the same access to end users via Windows as that

---

47. FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY, *supra* note 3.

48. *See* FTC Statement on Google/Doubleclick, *supra* note 36, at 2–3; Deborah Feinstein, *The Not-So-Big News About Big Data, Competition Matters Blog*, FTC (June 16, 2015), https://www.ftc.gov/news-events/blogs/competition-matters/2015/06/not-so-big-news-about-big-data [https://perma.cc/VP5T-DY5C] ("[T]he FTC has explicitly recognized that privacy can be a non-price dimension of competition.").

49. Makan Delrahim, Assistant Attorney Gen., Dep't of Just., Remarks for the Antitrust New Frontiers Conference (June 11, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers [https://perma.cc/4UKK-7WNN] ("[D]iminished quality is also a type of harm to competition. . . . [P]rivacy can be an important dimension of quality.").

50. Margrethe Vestager, Comm'r for Competition, Eur. Comm'n, Mackenzie Stuart Lecture at Cambridge: Making the Data Revolution Work for Us (Feb. 4, 2019), ("[I]f privacy is something that's important to consumers, competition should drive companies to offer better protection."); *see, e.g.*, Facebook/WhatsApp (Case No COMP/M.7217) Commission Decision C (2014) 7239 [2014], Eur. Comm'n, ¶ 174 (Mar. 10, 2014) (acknowledging privacy as a non-price element of competition); European Commission Press Release IP/16/4284, Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 [https://perma.cc/2YCQ-WRHG] (same).

51. Nat'l Soc'y of Pro. Eng'rs v. United States, 435 U.S. 679, 695 (1978) ("[A]ll elements of a bargain—quality, service, safety, and durability—and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers.").

52. Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 180 (Dec. 6, 2016).

53. *Id.*

afforded to LinkedIn. This was likely to cause a decline in the privacy options available for consumers as they selected from among different social networking services.[54] The merger decision recognizes that privacy is "an important parameter of competition . . . to the extent that consumers see it as a significant factor of quality."[55] European antitrust authorities imposed remedies on Microsoft as a condition of permitting the merger. The remedies sought to protect consumers from the anticipated privacy-quality harms, by ensuring that rival social media services could continue to interoperate with Windows, and thus to compete with LinkedIn.[56]

Under this theory of privacy quality for mergers, antitrust authorities account for evidence of a likely decline in privacy-based competition in their evaluation of the competitive effects of the proposed transaction. If those effects are substantial, antitrust authorities might seek to block the merger. But if the merger has little or no effect on privacy-based competition, then (assuming no other substantial effects on other parameters of competition) antitrust authorities will allow the transaction to proceed.[57]

More recently, privacy-as-quality theory has also begun to appear in high-profile monopolization cases against digital giants. Complaints against Google and Facebook allege these technology companies used their monopoly power to erode the quality of online data privacy. As part of a broader set of antitrust claims,[58] the DOJ alleges that Google used its market power to harm consumers by reducing search quality on "dimensions such as privacy, data protection, and use of consumer data."[59] In a groundbreaking case against Facebook, the FTC and several states allege the company used its market power in social networking to erode privacy quality.[60] The case centers on Facebook's pattern of acquisition or exclusion of

54. European Commission Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 [https://perma.cc/2YCQ-WRHG].

55. *Id.*

56. Eur. Comm'n, *Microsoft/LinkedIn*, *supra* note 50. To mitigate the privacy-related foreclosure concerns, the Commission required that Microsoft commit to limit the automatic installation of LinkedIn on Windows PCs, both at the manufacturer and end user level, and imposed protective measures to prevent Microsoft from retaliating against manufacturers who choose to install competing social networking applications. It also required Microsoft to provide commitments to ensure continued interoperability between Windows and competing professional social networking services, such as guaranteed competitor access to Microsoft APIs and Microsoft's Graph.

57. *See, e.g.*, FTC Statement on Google/Doubleclick, *supra* note 36, at 2.

58. The DOJ's primary contention is broader than just the privacy aspects of the case relevant here. The agency claims that Google foreclosed competition for online search through agreements that required Google to be the default, preloaded search engine on mobile phones and other search access points. Complaint, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020).

59. *Id.* ¶ 167 (alleging that by "restricting competition in general search services, Google's conduct has harmed consumers by reducing the quality of general search services (including dimensions such as privacy, data protection, and use of consumer data)"). A similar Colorado-led state case against Google claims that Google collects "more personal data about more consumers" than it would be able to in a competitive market. Complaint ¶ 98, Colorado v. Google LLC, No. 20- cv-03715 (D.D.C. Dec. 17, 2020).

60. Substitute Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Facebook, Inc., No. 1:20-cv-03590 (D.D.C. Sept. 8, 2021).

nascent competitors—called a "buy or bury" strategy—which the FTC claims is a violation of Section 5 of the FTC Act, a major federal antitrust law.[61] Facebook allegedly exercised its power over social media markets to offer "lower levels of service quality on privacy and data protection than it would have to provide in a competitive market."[62] Specifically, the agency claims that Facebook's conduct caused a decline in "consumer choice," including fewer data privacy protection options "regarding the amount and nature of advertising . . . the availability, quality, and variety of data protection privacy options for users [and] options regarding data gathering and data usage practices."[63] Broadly understood, both cases allege that privacy protection in the market would be stronger but for the alleged monopolization engaged in by these firms.

While the Facebook case is at the early stages, the Judge has adopted privacy-as-quality theory in early rulings. In a partial denial of Facebook's motion to dismiss, Judge James Boasberg of the District of Columbia found it plausible that consumers would prefer social networking services with more privacy-protective ad delivery mechanisms.[64] In the parallel state claims, he ruled that the states had standing based on privacy harm to their citizens, who experienced "reductions in the quality and variety of privacy options and content available to them in that [social media] market."[65] As these cases and complaints show, privacy-as-quality has become the primary theory—really, the only theory—of how antitrust law and data privacy law interact.[66]

C. So Far, So Easy: Shared Assumptions of Markets and Choice between Antitrust and Data Privacy Law

This prevailing privacy-as-quality theory offers a tidy and convenient reconciliation of privacy and antitrust law. It simply extends antitrust law assumptions about markets to data privacy, subsuming privacy into existing antitrust theory as a factor in competition.

Antitrust law is premised on the idea that, in the absence of anticompetitive

---

61. *Id.* ¶ 77. The FTC points to Facebook's acquisitions of social networking company Instagram and online messaging company WhatsApp, which it claims solidified Facebook's monopoly power in the market for personal social networking. *Id.* ¶ 129. The FTC's initial complaint against Facebook was dismissed, and this discussion refers to the FTC's second, amended complaint.

62. *Id.* ¶ 222.

63. *Id.* ¶ 221.

64. FTC v. Facebook, Inc., 581 F. Supp. 3d 34, 55 (D.D.C. 2022) (finding support for this conclusion in federal legislation that addresses "various privacy and advertising concerns related to consumer technology" and referencing as examples of such federal legislation 15 U.S.C. § 6101 et seq. (Telemarketing and Consumer Fraud and Abuse Prevention Act); 15 U.S.C. § 7701 et seq. (Controlling the Assault of Non-Solicited Pornography and Marketing Act); 47 U.S.C. § 227 (Telephone Consumer Protection Act).

65. New York v. Facebook, Inc., 549 F. Supp. 3d 6, 23 (D.D.C. 2021) (quoting the States' Redacted Complaint, ¶¶ 8, 247–50, and finding it plausible if "a shade vague"). The states' claims were dismissed on other grounds centering on laches—a delay in the government bringing their claim against Facebook.

66. Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON. 1, 2–3 (2015) (disagreeing with the approach of treating privacy as quality, but noting that the analysis of privacy as an element of quality is one of the most developed theories).

conduct, markets will function.[67] Consumers will make choices, competition will occur based on those choices, and this process will enhance consumer welfare. Antitrust enforcement combats anticompetitive mergers and conduct to enable markets to operate, to the presumed benefit of consumer welfare.[68]

As the Supreme Court explains, the Sherman Act makes a legislative judgment that competition is positive for consumers.[69] Even if that judgment is not correct in every market or situation, "the statutory policy precludes inquiry into the question [of] whether competition is good or bad . . . ."[70] This means courts applying antitrust law cannot decide to limit competition in the name of promoting other public policy interests such as public health, safety,[71] or even privacy, in ways that are not provided for by the legislation. For example, antitrust agencies have sought to promote competition among cigarette manufacturers by ensuring their mergers do not reduce competition, even though this helps to sell more products that are known to be damaging to public health.[72] The goal of antitrust law is to promote competition, not other public policy interests, even when those interests are unquestionably valid.

This pro-market view animates antitrust law throughout. Antitrust analysis focuses on market definition, barriers to market entry, competitors in the market, and, ultimately, effects on competition within the relevant market(s). The suggestion here is not that this should, or even could, change. Instead, it offers this explanation of the antitrust view of the world as market driven. This extends to how antitrust views data privacy.

This market orientation in antitrust law drives two related assumptions that are essential to privacy-as-quality theory. First, antitrust assumes that the parameters of competition—including privacy—can be understood in price-equivalent terms. To be accounted for in antitrust analysis, whatever is being considered is framed in terms of price or price-equivalency. For example, Judge Boasberg found the states have standing in their case against Facebook because of:

---

67. D. Daniel Sokol, *Antitrust, Institutions, and Merger Control*, 17 GEO. MASON L. REV. 1055, 1062 (2010) ("The basis for antitrust enforcement is the belief that markets work."); HERBERT HOVENKAMP, THE ANTITRUST ENTERPRISE: PRINCIPLE AND EXECUTION 7 (2005) (describing antitrust as "a type of market intervention in an economy whose nucleus is private markets").

68. *See, e.g.*, Herbert Hovenkamp, *On the Meaning of Antitrust's Consumer Welfare Principle*, CONCURRENTALISTE (Jan. 17, 2020).

69. Nat'l Soc'y of Pro. Eng'rs v. United States, 435 U.S. 679, 695 (1978).

70. *Id.* at 695–96.

71. *Id. See similarly* FTC v. Superior Court Trial Lawyers Assn., 493 U.S. 411, 423–24 (1990) (refusing to consider whether the restraint of trade among criminal defense lawyers served a social good more important than competition: "The social justifications proffered for respondents' restraint of trade . . . do not make it any less unlawful").

72. *See, e.g.*, Reynolds American Inc. and Lorillard Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 80 Fed. Reg. 32374 (June 8, 2015) (challenging proposed merger that would reduce competition between major cigarette companies).

> "reductions in the quality and variety of privacy options and content available to [the states' citizens]" . . . which is to say that, on the States' theory, millions have experienced a rise in the effective price of using Facebook, [as] users "exchange their time, attention, and personal data for access to Facebook's services."[73]

This treats privacy as "price-equivalent"; less privacy is equivalent to paying a higher price for social media services.

Second, antitrust assumes that consumer choices will drive competition. Antitrust law often emphasizes, as a shorthand for the competitive process, the importance of "consumer choice" in markets. Competition between firms is thought to push companies to offer more and better products and services to consumers, increasing consumer options within the marketplace.[74] Antitrust law combats anticompetitive conduct and mergers that reduce this array of consumer choices available in markets.[75]

Antitrust law assumes that consumers are able to make informed choices between the products and services offered by businesses, selecting based on their preferences for price, innovation, service, and quality. The expectation is that this choice, in competitive markets, will discipline weak or bad actors. Consumers will move their business away from these bad actors to other firms that provide a more desirable mix of features in their product or service offerings. Firms that fail to provide such offerings lose out to rivals and may eventually exit the market.

The theory of privacy-as-quality extends this assumption to competition that is based on data privacy. It takes for granted that consumers can make privacy choices consistent with their preferences in markets. The expectation is that, in the absence of anticompetitive conduct, consumers will switch to products and services that offer their desired level of privacy protection, abandoning the businesses that fail to protect their privacy in the way that consumers want. For example, the FTC's recent case against Facebook claims that the company is able to extract more personal data from consumers because there are few or no firms to which

---

73. New York v. Facebook, Inc., 549 F. Supp. 3d 6, 23 (D.D.C. 2021) (internal quotations omitted, emphasis in original) (quoting the States' Redacted Complaint, ¶¶ 8, 247–50, and finding it plausible if "a shade vague").

74. *See, e.g.*, *Competition Policy*, EUR. COMM'N, https://competition-policy.ec.europa.eu/about/why-competition-policy-important-consumers_en [https://perma.cc/7ZB4-2L5R] (last visited Apr. 11, 2024) (noting competition policy in Europe "creates a wider choice for consumers").

75. *See, e.g.*, *Mergers and Competition*, FTC, https://www.ftc.gov/news-events/topics/competition-enforcement [https://perma.cc/W7A9-SDVU] (last visited Apr. 11, 2024) ("Competition in America benefits consumers by keeping prices low and the quality and choice of goods and services high, and makes our economy work. . . . The FTC promotes competition, and challenges anticompetitive business practices and mergers, to make sure that consumers have access to quality goods and services, and businesses can compete on the merits."); Paul Nihoul, *"Freedom Of Choice": The Emergence Of A Powerful Concept In European Competition Law*, *in* CHOICE: A NEW STANDARD FOR COMPETITION ANALYSIS? 10, 10–21 (Paul Nihoul, Nicolas Charbit & Elisa Ramundo eds., 2016) (tracing the role of consumer choice considerations in EU competition decisions).

consumers could switch for social networking services, if those consumers prefer stronger privacy protections than those offered by Facebook's services.[76] If there were more competition for online social networking, the assumption is that Facebook would be pressed into offering better privacy protections by the risk of competitors winning away its users with more privacy-protective services.[77] If the anticompetitive conduct is eliminated through antitrust enforcement, the unstated assumption is that privacy-related market forces will prevail. Privacy-based competition will be restored, consumers will resume making privacy choices consistent with their preferences, and will see better privacy protection as a result.

At least until recently, this was a fair, and shared, market assumption between antitrust law and the bulk of U.S. data privacy law. Data privacy law has long assumed that, absent misconduct, consumers will make choices about their privacy in the market. For decades, U.S. federal privacy law has centered on "notice and consent," a mechanism that places the onus on individuals to make choices about their privacy.[78] Under a notice and consent (or sometimes "notice and choice") regime, companies are obligated to tell individuals about their personal information collection, use, and disclosure practices ("notice"), then provide those individuals with a "choice" to consent to the terms of use in the notice or to refuse consent, often by not using the good or service.[79] Provided this notice and consent occurs, U.S. federal privacy law leaves firms largely free to collect and use personal data in any way that is consistent with that notice.[80]

Notice and consent remains the lynchpin of sectoral privacy laws enacted in

---

76. Substitute Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 105, 127, FTC v. Facebook, Inc., No. 20-cv-03590 (D.D.C. Sept. 8, 2021) (arguing that Facebook's acquisition of Instagram and WhatsApp deprived consumers of more privacy-protective options in the relevant market); *see also* Bundeskartellamt v. Facebook, B6-22/16, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html [https://perma.cc/U3NG-D YM9] (Ger.).

77. *See, e.g.*, U.K. Competition & Markets Auth., Online Platforms and Digital Advertising Market Study, at 181 (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study [https://perma.cc/HM27-WP8M] ("If there were more choice for consumers, then there could be scope for more competition between platforms as platforms would need to compete more actively to persuade consumers of the benefits of personalised advertising. There would also be scope for other platforms to compete for consumers on the basis of alternative business models offering different options in respect of the privacy choices and the services that they offer.").

78. The notice and consent paradigm is often traced back to the Fair Information Practice Principles, articulated by the U.S. Department of Health, Education, and Welfare in the early 1970s. The FIPs or FIPPs reached far beyond their health-specific origins to shape U.S. privacy law and the FTC's approaches to it under Section 5 and sectoral law. The FIPs emphasize each individual's interest in receiving notice of data gathered about themselves and the right to consent to the collection and use of their personal data. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41–42 (1973).

79. *Id.*

80. Daniel J. Solove & Paul M. Schwartz, *American Legal Institute Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1252, 1269 (2022) (describing basics of the notice and consent approach to U.S. law).

the 1990s, such as the Children's Online Privacy Protection Act,[81] the Health Insurance Portability and Accountability Act,[82] and others. These federal statutes require notice and consent in specified circumstances as a condition of lawful collection and use of personally identifiable information.[83] Notice and consent remain the backbone of the U.S. approach to privacy law,[84] though, as Part III of this Article demonstrates, this is beginning to change in significant ways.[85]

The other important sources of U.S. federal privacy law, Section 5 of the FTC Act, also center on consumer choice. As mentioned above, the FTC, at the urging of Congress, has used its general consumer protection authority under Section 5 of the FTC Act to protect individuals from a myriad of data privacy abuses. When companies fail to offer individuals meaningful opportunities to consent to personal data use, they risk Section 5 FTC enforcement for unfair or deceptive practices. Section 5 is a consumer protection law; it mentions privacy zero times in its statutory text.[86] But since the mid-1990s, the FTC has been enforcing Section 5 against companies who engage in false or misleading promises regarding the collection, use, and sale of consumers' personal data in what has become the *de facto* common law of data privacy.[87]

Section 5 empowers the FTC to prevent unfair and deceptive acts or practices in the marketplace.[88] The agency brings most of its privacy cases under the deception branch of Section 5, which prohibits misrepresentations, omissions, or other practices that mislead a consumer who is acting reasonably in the circumstances, to the consumer's detriment.[89] To be actionable, a deception must be "material," which is defined as "likely to affect a *consumer's choice* of or conduct regarding a product."[90] In its data privacy cases, the FTC uses this prohibition against companies that fail to uphold the representations made in their privacy

81. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505.

82. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 201–264.

83. *See, e.g.*, 15 U.S.C. § 6502 (requiring operators to "[p]rovide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information" and "obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children"); Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. §164.520(a)(1) (2011) ("[A]n individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity . . . ."); *Id.* § 164.506(b)(1) ("A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.").

84. Solove & Hartzog, *supra* note 16, at 593.

85. *See infra* Part III. The Changing Character of U.S. Data Privacy Law and its Impacts on Antitrust Theory.

86. 15 U.S.C. § 45(a)(1) (2018).

87. Solove & Hartzog, *supra* note 16, at 598–600.

88. 15 U.S.C. § 45(a)(1).

89. Solove & Hartzog, *supra* note 16, at 638 (noting the FTC has primarily used its deception authority but confirming "trend of judicious yet increasing pleading of unfairness" by the agency).

90. Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1984) (emphasis added), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/9N38-VFZ6] (appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984)).

policies, or that fail to adequately disclose how personal data is used.[91] Both deprive consumers of the choices they would ordinarily have had the opportunity to make in the market. Had the consumer known that the company would fail to keep its privacy promises or how their data would actually be used, in theory, that consumer could have chosen other services.[92] The concept of consumer choice thus plays a central role in the FTC's privacy deception cases.

This choice-centric thinking also appears in the other branch of Section 5, the prohibition on "unfair" acts or practices. The FTC explains in its policy guidance on unfairness cases that:

> Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory.[93]

Based on this view, the FTC uses its unfairness authority to intervene when misconduct "prevent[s] consumers from effectively making their own decisions."[94] In the realm of data privacy, this has meant complaints challenging retroactive changes to privacy policies, deceitful data collection, and the improper use of data or unfair design practices that obstruct consumers from exercising their choices.[95]

The assumption is that if the FTC intervenes to end unfair or deceptive practices through Section 5 enforcement, consumers will resume making privacy choices consistent with their preferences. In its interventions, the FTC makes clear that its purpose is "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making."[96] Section 5 combats deceptive and misleading practices *so that* consumers can choose. Applied to the privacy-related enforcement of Section 5, this amounts to an assumption that, in the absence of misconduct, the markets for data privacy work—much like the assumption made by antitrust law.

---

91. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief at 19, FTC v. Frostwire, LLC, No. 11-cv-23643 (S.D. Fla. Oct. 12, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [https://perma.cc/27LL-T24M] (alleging deception based on a failure of Frostwire to adequately disclose default public sharing of user files by its software).

92. FTC Policy Statement on Deception, *supra* note 90 ("Deceptive practices injure both competitors and consumers because consumers who preferred the competitor's product are wrongly diverted.").

93. Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 19, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [https://perma.cc/2KQL-A7MA].

94. The FTC has also brought privacy-related cases under the "unfair[ness]" branch of Section 5, which permits agency action when an act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." *See* FTC Policy Statement on Unfairness, *supra* note 93.

95. Solove & Hartzog, *supra* note 16, at 640 (summarizing the categories of FTC unfairness cases relating to privacy).

96. FTC Policy Statement on Unfairness, *supra* note 93.

In sum, data privacy law has often shared an important commonality with antitrust law: the assumption that consumers will make choices consistent with their preferences in the market. The choice-centric data privacy laws, which emphasize notice and consent by consumers, make for a tidy reconciliation with antitrust law. Both areas of law pursue misconduct that impairs consumers' ability to choose in the market, on the premise that such choice will improve the lot of consumers by giving them more privacy, and more competition. As the acting head of the FTC observed this commonality means that a "dearth of real [consumer] choice is a privacy problem, but it is also a competition problem."[97] This paradigm of data privacy law creates a cohesive legal and policy landscape with antitrust, in which each doctrinal area can pursue its respective enforcement goals without any question of which to prefer. It is tidy, and it works—but not for long. As the remainder of this Article explains, privacy-as-quality theory offers an increasingly incomplete antitrust answer to the evolving world of data privacy law.

II. THE CONSEQUENCES OF NARROW PRIVACY PARADIGMS IN ANTITRUST LAW*:* UNEXAMINED PRIORITIZATION OF COMPETITION OVER DATA PRIVACY

This Article contends that antitrust theory has failed to account for the complexities of modern privacy law. Before reaching that argument, there is an important preliminary question: Does it matter if antitrust fails to understand data privacy? After all, each is a separate area of law with its own goals. Perhaps their intersection should simply be left at the *status quo*?

This Part argues it does matter. At a basic level, it matters that antitrust law has theories that are correct and useful where it overlaps with privacy. Good law is always a good idea. But thin conceptions of privacy in antitrust matter for two less obvious reasons as well. First, existing theory predisposes privacy interests to be subordinated to competition interests, often without examination or justification. Second and relatedly, the freewheeling development of the common law means that thin conceptions of data privacy in antitrust law may infect and undermine privacy law itself.

In a growing array of cases, competition interests are squaring off against privacy interests. For example, defendants in antitrust cases have successfully argued that the foreclosure of competitors from popular digital platforms is necessary to protect end users' data privacy.[98] In the legislative context, bills propose that digital platform operators be required to provide those same competitors with the ability

97. *Hearings on Competition and Consumer Protection in the 21st Century, Hearing No. 12: The FTC's Approach to Consumer Privacy*, Fed. Trade Comm'n 131 (Apr. 10, 2019) (remarks by Rebecca Kelly Slaughter, FTC Comm'r), https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf [https://perma.cc/6ZWN-3QDK].

98. Epic Games, Inc. v. Apple Inc., 559 F. Supp. 3d 898, 1002-06 (N.D. Cal., 2021) (affirming the District Court finding that Apple established a justification for its conduct based on privacy competition), *aff'd*, 67 F.4th 946 (9th Cir. 2023); hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1189 (9th Cir. 2022), *order dissolved*, No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022); *see also* international cases such as Comm'r of Competition v. Toronto Real Est. Bd., 2016 Comp. Trib. 7 CT-2011-003, 74 (Can.).

to interoperate with such platforms.[99] This interoperability would mean access to personal data, yet these bills pay little attention to privacy. Each of these situations require policy or legal choices between data-driven competition and the restraints on data processing that are demanded by privacy law.

In these scenarios, existing antitrust conceptions of privacy set the stage for courts and legislators to take a "competition first" view of any tradeoffs with data privacy. Privacy-as-quality theory treats privacy as a subsidiary factor in competition analysis. Competition becomes paramount, at least in part because the conceptualization of data privacy is so narrow within this theory. It may be that competition is, in fact, preferable in some situations. But that priority should be a conscious and carefully reasoned choice in broader policy and law rather than just a side effect of underdeveloped antitrust theory of privacy.

This competition primacy is emerging in early judicial decisions where courts are asked to choose between privacy and competition. In *hiQ Labs, Inc. v. LinkedIn Corp.*, both the District Court[100] and the Ninth Circuit[101] were quick to emphasize the plaintiff's interests in competition over the privacy interests invoked by the defendant. HiQ is a data analytics company that sells "people analytics" software used mainly by employers.[102] Its software is powered by collecting ("scraping") data from the LinkedIn social network profiles of individuals, such as their names, job titles, work history, skills, and evidence of changes to their profile.[103]

LinkedIn initially permitted hiQ to access user data on its social network service but later blocked hiQ from the LinkedIn servers.[104] HiQ brought claims of exclusionary conduct under state antitrust law against LinkedIn, seeking to restore its data access.[105] It argued that LinkedIn's termination constituted unfair competition in

99. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/2992 [https://perma.cc/2TP3-NFYB].

100. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1117 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019), *cert. granted*, *judgment vacated*, 141 S. Ct. 2752 (2021), *aff'd*, 31 F.4th 1180 (9th Cir. 2022). The case was appealed and remanded on questions unrelated to the discussion here that focused on preemption of the state claims by the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (hiQ sought a declaratory judgment that the Computer Fraud and Abuse Act did not apply to its conduct after LinkedIn had threatened to invoke it). The 2019 and remanded 2022 Ninth Circuit decisions are also virtually identical on the privacy and competition topics discussed here. *hiQ Labs*, 31 F.4th at 1187.

101. *hiQ Labs*, 31 F.4th at 1190.

102. *hiQ Labs*, 31 F.4th at 1187.

103. *Id.* at 1187.

104. *Id.* at 1192–93.

105. *Id.* at 1188. HiQ brought suit under California Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200 et seq., among other causes of action. However, hiQ's argument was very similar to a Section 2 Sherman Act refusal-to-deal claim in federal law. In fact, the District Court looks to Section 2 of the Sherman Act for guidance on what constitutes an anticompetitive act in state law. *hiQ*, 273 F. Supp. 3d at 1117. Although the Ninth Circuit did not reach the unfair competition claim (because the tortious interference with contract claim was sufficient to uphold the injunction), the Court's consideration of the tort claim included analysis of whether interference was "within the realm of fair competition" and whether there was a plausible justification for the conduct in tort law. *hiQ*, 31 F.4th at 1193–94.

service of LinkedIn's own plans to introduce competing data analytics software.[106]

To defend against hiQ's claims, LinkedIn invoked its users' privacy interests.[107] LinkedIn argued that hiQ was violating data privacy by disregarding user profile settings. hiQ was gathering data from the profiles of individuals and using it to notify anyone who purchased hiQ software when those individuals made updates to their LinkedIn profile—even if that person had opted out of broadcasting such changes to their network, by using LinkedIn's privacy settings.[108] LinkedIn is commonly used for professional networking.[109] Changes to user profile information can indicate an impending job search and employee departure. In fact, that was the premise of hiQ's software—alerting employers to which of their employees are at risk of leaving their job, based on changes to the employee's LinkedIn profile.[110] Understandably, individuals might want to avoid advertising profile changes and a related job search if their professional network includes their employers. LinkedIn argued that individual users had purposefully engaged a privacy setting called "do not broadcast," which prevented such changes to their online profile from being broadcast out to their professional social network via an automatic email.[111] Regardless of whether individuals had engaged the "do not broadcast" setting, hiQ was reporting profile changes to employers.[112] This ignored user settings and also violated LinkedIn's terms of service.[113]

The District Court as well as the Ninth Circuit were skeptical that individuals had any privacy interests in their public social media profiles.[114] The District Court declared that such privacy interests were "at best uncertain."[115] Even if users had privacy interests in their LinkedIn data, the courts in *hiQ Labs v. LinkedIn* agreed that such interests were outweighed by hiQ's interest in continuing its business.[116] In balancing the harms at stake, the Ninth Circuit affirmed that "even if some users retain some privacy interests in their information" despite it being made public, those interests were not significant enough to outweigh hiQ's interest in continued

106. *hiQ*, 31 F.4th at 1193.

107. *Id.* at 1189.

108. *Id.* at 1189–90.

109. *About LinkedIn*, LINKEDIN (March 20, 2024), https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl [https://perma.cc/S39A-6Z4Z] (describing LinkedIn as "the world's largest professional network").

110. *hiQ*, 31 F.4th at 1187 (describing hiQ's products).

111. An estimated fifty million LinkedIn users chose to engage the "Do Not Broadcast" setting. Once the setting was activated, changes made by the user to their profile were no longer sent via automated e-mail from LinkedIn to the contacts in the user's LinkedIn social network. When the setting was not engaged, everyone in the user's network received an automated alert highlighting the changes in their profile. *Id.* at 1189.

112. *Id.*

113. *Id.* at 1190.

114. *Id.* (finding "little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy" in such information); hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1119 (N.D. Cal. 2017).

115. *hiQ*, 273 F. Supp. 3d at 1119.

116. *hiQ*, 31 F.4th at 1190.

access to the users' data to run its business, at least at the preliminary injunction stage.[117] At times, the Ninth Circuit also seems concerned with the broader effects on competition that could arise were the law to permit companies like LinkedIn, whose servers hold vast amounts of public data, to "selectively" ban potential competitors from access to that data.[118] It observed that granting such power "risks the possible creation of information monopolies that would disserve the public interest."[119]

The Ninth Circuit ultimately upheld the preliminary injunction requiring LinkedIn to restore hiQ's access to consumer profile data.[120] The injunction required LinkedIn to remove any existing technical barriers to hiQ accessing public user profiles, and to refrain from putting in place any legal or technical measures with similar effect.[121]

The *hiQ Labs v. LinkedIn* litigation illustrates the problem of weak recognition of privacy interests in antitrust cases. The District Court found it "unlikely" that "most users' actual privacy expectations are shaped by the fine print of a privacy policy buried in the User Agreement that likely few, if any, users have actually read."[122] This view flies in the face of data privacy law. The FTC's Section 5 enforcement is rooted in exactly the opposite premise—that consumers' reasonable expectations of privacy are based on the promises companies make in their privacy policies.[123]

The Ninth Circuit was similarly skeptical that any privacy interests were at stake[124] but instead emphasized LinkedIn's privacy policy, and the public nature of social media posts, to support this conclusion.[125] It observed that the privacy policy puts users on notice that their information could be seen by others.[126] The Ninth Circuit concluded that this warning and the public nature of the data make it unlikely that "LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly."[127] This was, in part, an evidentiary problem, as the Court found LinkedIn lacked evidence of the asserted user privacy interests.[128] Still, the Ninth Circuit was quick to synonymize public disclosure of data on social media with the elimination of all

---

117. *Id.*; *hiQ*, 273 F. Supp. 3d at 1107 (finding the balance of hardships tips "sharply" in hiQ's favor).

118. *hiQ*, 31 F.4th at 1194.

119. *Id.* at 1202.

120. *Id.* at 1202–03. The order issued in this decision was later dissolved, as hiQ was no longer actively operating its business. Order, hiQ Labs, Inc. v. LinkedIn Corp., No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022).

121. *hiQ*, 31 F.4th at 1188.

122. *hiQ*, 273 F. Supp. 3d at 1107.

123. *See* Solove & Hartzog, *supra* note 16 (describing the FTC's initial approach of enforcing privacy "promises" made by companies).

124. *hiQ*, 31 F.4th at 1194 (agreeing with the District Court that user privacy expectations in all public LinkedIn profile information were "uncertain at best").

125. *Id.* at 1190.

126. *Id.*

127. *Id.*

128. *Id.* (finding "little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy" in such information); *hiQ*, 273 F. Supp. 3d at 1107 ("LinkedIn has presented little evidence of users' actual privacy expectation.").

privacy interests in that data. Further reflecting this minimization of privacy interests, the injunction itself makes no mention of consumer data privacy, privacy settings, or how data privacy might be accommodated within the terms of hiQ's access.[129]

This constrained view of data privacy in *hiQ Labs v. LinkedIn* falls short of privacy law's own conceptions of protected interests. While recognizing that there may be less privacy protection for data that is made public, a choice to disclose certain data does not necessarily equate to the elimination of all control over unauthorized access to that data.[130] Yet *hiQ Labs v. LinkedIn* casts the privacy interests as uncertain, limited, and comparatively unimportant to the competition interests of the plaintiff. This limited judicial conception of privacy interests leads directly to the conclusion that such privacy interests are "sharply" outweighed by the interests in competition.[131] In short, the LinkedIn courts easily prefer competition over data privacy.

Although *hiQ Labs v. LinkedIn* is an early decision on the tradeoffs between privacy and competition, it demonstrates several reasons why judicial preferencing of competition over privacy is likely to continue. Many data privacy harms are weakly established in the law relative to antitrust harms recognized in antitrust law.[132] As scholars Solove and Citron aptly summarize, privacy harms often involve an increased risk of future harm—such as inaccurate credit reporting, which can create economic and reputational harm—which the law struggles with because that harm is inchoate and not necessarily concrete.[133] This has meant that the FTC and private plaintiffs face serious challenges in demonstrating that privacy harms are concrete and recognized by the law. The FTC has lost cases where it alleged harms to privacy that were inchoate or nonfinancial in nature, such as the risk of identity theft.[134]

Relatedly, the nature of privacy harms often makes those harms difficult to quantify and to substantiate with adequate evidence. Privacy harms often involve

---

129. *See hiQ*, 273 F. Supp. 3d at 1099 (granting hiQ's motion for a preliminary injunction and setting out the terms of the Order).

130. *See, e.g.*, NISSENBAUM, *supra* note 19 at 119 (challenging the public/private dichotomy as the basis for understanding privacy protection, in particular for social networking sites "that, for now . . . seem to defy obvious categorization as either public or private.").

131. *hiQ*, 273 F. Supp. 3d at 1108.

132. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1090 (2002) ("Privacy problems are often not well articulated, and as a result, we frequently do not have a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems.").

133. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 816–818 (2022) (observing that "privacy harms present several challenges that make their recognition [in law] difficult" and describing the tendency of privacy harms to involve future risks); *see also* TransUnion LLC v. Ramirez 594 U.S. 413, 417 (2021).

134. *See, e.g.*, Fed. Trade Comm'n v. D-Link Sys., Inc., No. 17-CV-00039, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017) (dismissing an FTC claim that failed to allege consumer injury "in the form of a monetary loss"); In the Matter of LabMD, Inc., No. 9357, 2015 WL 7575033, at *41–43 (MSNET Nov. 13, 2015) (dismissing a section 5 FTC Act complaint for failure to allege that the data security breach resulted in, or was likely to result in, consumer injury such as identity theft and reputational or other similar harms), rev'd, 2016-2 Trade Cas. (CCH) (MSNET July 28, 2016), *aff'd on other grounds*, LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

many small incursions that can be challenging to quantify for each person but that occur on a large scale that makes them societally harmful when considered in the aggregate. These challenges are on display in *hiQ Labs v. LinkedIn*, where LinkedIn had difficulty both pleading and proving the privacy harms it asserted.[135] The courts expressed a surprising degree of doubt that any privacy interest could exist in public profile data on social media.

In contrast, harms to competition are often more concrete, more easily evidenced, and have a more established history in the law than data privacy harms. Competition harms are more readily recognized in law because of their economic, price-based nature, which often makes them tangible and concrete. Competition harms are also easier to evidence—antitrust cases are notorious for their extensive economic experts, models, and documentary evidence.

This leaves competition harms poised to prevail over data privacy harms. Privacy harms will often be afforded little weight against more readily established harms to competition. Scholar Julie E. Cohen observes that when privacy is weighed against economic efficiency or entrepreneurship, the result is likely to be that "privacy comes up the loser."[136] Daniel Solove makes a similar observation, albeit outside of the antitrust context, that other interests like free speech or data security are often more readily articulated when balanced with data privacy and thus weighed heavily against ill-defined data privacy harms.[137] For all of these reasons, the antitrust judiciary is likely to find competition harms more easily identifiable and more substantial than privacy harms.

Taken one step further, these frail conceptions of privacy within antitrust could infect the common law of data privacy itself. This risk should be of particular concern for data privacy practitioners and scholars. The nature of the common law means that thin conceptions of privacy in antitrust cases like *hiQ Labs v. LinkedIn* are not cabined to antitrust doctrine. Antitrust cases have begun to make broad declarations about the bounds of data privacy without necessarily understanding the nuances of privacy doctrine. For example, in *hiQ Labs v. LinkedIn,* both the District Court and Ninth Circuit doubted the existence of any privacy interests once data is made public on social media.[138] Such decisions, when taken as precedent wherever the common law leads, may bleed into broader privacy doctrine.

Such development of the common law could further impair the already-fragile recognition of harms in privacy law itself. Decisions could pick up on these threads

---

135. *See* hiQ, 273 F. Supp. 3d at 1106 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985, 994 (9th Cir. 2019), cert. granted, judgment vacated on other grounds, 141 S. Ct. 2752 (2021), *aff'd*, 31 F.4th 1180 (9th Cir. 2022), order dissolved, No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022).

136. Julie E. Cohen, *What Privacy is for*, 126 HARV. L. REV. 1904, 1904 (2013).

137. SOLOVE, *supra* note 11, at 7–8; *See also* NISSENBAUM, *supra* note 19 at 111 (observing the conflict between privacy and countervailing interests in security, free speech and efficiency, and finding that "as long as privacy's social value is ignored, we are likely to see it consistently, and mistakenly, undervalued.").

138. hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1190 (9th Cir. 2022) (agreeing with the District Court that there is "little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy" in such information).

of privacy in antitrust law and use them to weaken the common law on privacy interests. The statements in *hiQ Labs v. LinkedIn* would be convenient for use in later privacy cases that seek a narrow interpretation of privacy interests in public profile data on social media. In this sense, judicial perceptions of data privacy within antitrust are not just an antitrust problem—they may strike back to become a problem for data privacy law as well.

This very concern—that antitrust law may get privacy "wrong," to the detriment of privacy law itself—emerged in a recent high-profile decision by a top European Court. In July 2023, the European Court of Justice (ECJ) ruled on the appeal of a case brought by German competition enforcers against Facebook (now Meta).[139] The original decision found that Facebook's tracking of users on websites other than its own violated the General Data Protection Regulation (GDPR), the primary EU privacy law, and thus also constituted an abuse of dominance in antitrust law. The theory of liability thus crossed over between the two areas of law in a novel way, invoking noncompliance with privacy law as evidence of an antitrust violation.[140]

The ECJ ruled that antitrust authorities in EU member states have the authority to determine whether a company violated privacy law as part of their assessment of an abuse of dominance (or "monopolization," as it is called in the United States).[141] This power reflects the new commercial reality in which personal data has "become a significant parameter of competition" and thus relevant to antitrust law.[142] However, the Court expressed concern for ensuring consistency between *antitrust* conceptions of privacy law and those in privacy law itself when this power is exercised by competition authorities.[143] In an effort to achieve such consistency, it placed two important limits on the power of antitrust authorities to draw conclusions on privacy law. First, the antitrust authority must ascertain whether the privacy misconduct it is considering, or similar misconduct, is already the subject of a decision by the relevant privacy authority.[144] If so, the antitrust authority cannot depart from that privacy law in its own assessment.[145] Second, antitrust authorities owe a duty of "sincere cooperation" with privacy authorities on such cross-doctrinal matters.[146] The case imposes these substantive and procedural protections because, without them, antitrust law may come to different conclusions about privacy protections and violations than those reached in standalone privacy

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

140. This discussion is not endorsing the German enforcer's theory that a violation of privacy law can amount to an abuse of dominance or arguing that the same conclusion would necessarily be reached in U.S. antitrust law. The case theory raises important, unanswered questions about the causal relationship, if any, between market power and the privacy violation.

141. Case C-252/21, Meta Platforms, Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 62 (July 4, 2023).

142. *Id.* ¶ 51.

143. *Id.* ¶ 52 (noting the need to ensure the consistency of application of privacy regulations).

144. *Id.* ¶ 56.

145. *Id.* While bound by the privacy law the antitrust authority remains free to draw its own conclusions on the relevance of any violations to the antitrust analysis. *Id.*

146. *Id.* ¶ 62.

law. It illustrates that, in the new interactions between antitrust and privacy, such inconsistencies have the potential to undercut, or at least confuse, privacy law itself.

Back in the United States, the tendency to prefer competition over privacy is not just discernable in the common law—it appears in legislation as well. As discussed above, the FTC uses its authority under Section 5 of the FTC Act as a tool to combat violations of data privacy. To establish a violation of the unfairness branch of this provision, the act or practice must "not [be] outweighed by countervailing benefits to consumers *or to competition*."[147] Under this *de facto* privacy law, benefits from competition are thus expressly permitted to outweigh harm from unfair privacy practices. The statute does not even require that the competition harms be quantifiably "greater"—just that they "outweigh" the privacy-related unfairness in some way, perhaps as a policy priority.[148] Since competition harms are easier to prove than privacy harms, as discussed above, competition benefits may often outweigh privacy harms. When the FTC brings privacy cases, it may not be able to establish that the practice is unfair in the face of countervailing competition interests. It could also influence the FTC into choosing not to bring privacy cases where there appear to be such competition interests. The primacy of competition is built into the statutory formulation of the law being used to protect data privacy.

This preference for competition over privacy also appears in a flurry of proposed antitrust legislation.[149] These bills seek to restore competition in digital ecosystems through mandated interoperability that would require large digital companies to allow third parties to interconnect with their online platforms for social media, search and e-commerce.[150] This access is meant to enable third parties, such as sellers on Amazon, apps on Facebook, or advertisers on Google, to reach end users through the large digital platform on equivalent terms to Amazon, Facebook or Google's own goods or services. Such mandated interoperability is intended to help nascent companies gain a foothold in digital competition, in hopes they can challenge the monopolies held by large digital platform operators.

In their fervent pursuit of digital competition, though, many of these bills pay little attention to the security and privacy implications of mandated interoperability. The bills impose broad interoperability obligations on large digital companies,[151] but

147. 15 U.S.C. § 45(n).

148. *Id.*

149. American Choice and Innovation Online Act, H.R. 3816, 117th Cong. (2021–2022); American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021–2022); Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, H.R. 3849, 117th Cong. (2021–2022); Open App Markets Act, S. 2710, 117th Cong. (2021–2022).

150. *See* bills referenced at footnote 149.

151. *See, e.g.*, American Innovation and Choice Online Act, H.R. 3816, 117th Cong. § 2(b)(1) (2021–2022) (making it unlawful for a covered platform to "restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features that are available to the covered platform operator's own products, services, or lines of business"); American Innovation and Choice Online Act, S. 2992, 117th Cong. § 2(c)(I) (2021–2022) (similar prohibition with the addition that the restriction may not "materially" restrict or impede).

they include only narrow, ill-defined data privacy and security exceptions.[152]

For example, Senator Amy Klobuchar's leading bill, the American Innovation and Choice Online Act, prohibits covered platforms from "materially restrict[ing] or imped[ing] the capacity of a business . . . to access or interoperate with the same platform, operating system, hardware or software features" that are made available to businesses that the platform itself owns.[153] Amazon Marketplace, for example, would have to provide merchants selling through its platform with the same data and access it gives to Amazon's own (in-house) products.[154]

The platforms are then afforded a defense or exception—they can refuse interoperability to protect "user privacy" or "the security of non-public data" (or the platform itself), but only if the refusal is "narrowly tailored, could not be achieved through a less discriminatory means, [is] non-pretextual, and [is] reasonably necessary."[155] Privacy is referenced by a single word alone—the concept is not defined or discussed anywhere else in the proposed legislation. Given the many potential conceptions and understandings of data privacy, this leaves the scope of the defense quite unclear.

The effect of these proposed laws is to shift the risk calculus of platforms, making them more likely to allow interoperability at the cost of data privacy. Under existing antitrust law, interoperability obligations are minimal.[156] Even dominant platforms are largely free to terminate third party access if such interoperation poses privacy or security risks. Apple has famously done so for its online app store, refusing to distribute any apps that fail to observe its strict privacy and security rules.[157] But proposed laws like Senator Klobuchar's will affect the likelihood that a platform terminates a third party for privacy reasons by heightening the risk of an antitrust law violation. If a third party engages in suspect privacy practices, the

---

152. American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(b)(I) (2021–2022) (allowing a defense for privacy or security only where "narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary"); American Innovation and Choice Online Act, S. 2992, 117th Cong. § 3(b)(2)(B)(ii) (2021–2022) (affirmative defenses) (same).

153. American Innovation and Choice Online Act, S. 2992, 117th Cong. § 2(b)(I) (2021–2022).

154. Amazon Marketplace is a popular online commerce platform owned and operated by Amazon. Both Amazon itself and third-party merchants sell to end consumers through the platform. *See* Dana Mattioli, *Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products*, WALL ST. J., (April 23, 2020), https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015 [https://perma.cc/5254-RYZA] (describing Amazon's business model).

155. American Innovation and Choice Online Act, S. 2992, 117th Cong. § 2(c) (2021-2022) (affirmative defenses).

156. Antitrust cases have imposed some duty to deal on monopolists where a prior profitable, voluntary relationship was terminated. Otherwise, even monopolists are generally free to choose their trading partners in U.S. antitrust law. *See* Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585 (1985); Verizon Commc'ns Inc. v. Law Offs. of Curtis V. Trinko, L.L.P., 540 U.S. 398, 408 (2004); Erik Hovenkamp, *The Antitrust Duty to Deal in the Age of Big Tech*, 131 YALE L.J. 1483, 1487 (2022) (describing narrow exceptions and stating that "[t]he default rule is that a firm can lawfully refuse to deal with rivals, so long as this choice is unilateral").

157. *See* Epic Games, Inc. v. Apple Inc., 559 F. Supp. 3d 898 (N.D. Cal., 2021), *aff'd.*, 67 F.4th 946, 985–86 (9th Cir. 2023).

platform operator risks liability under such laws if it terminates the access of that privacy bad actor. Why gamble with liability under the proposed legislation, given the narrowness of the privacy and security defense? This takes away the stick of easy third-party termination, which can be used to maintain user data privacy and security on large digital platforms. These bills pursue competition at some cost to platforms in upholding data privacy standards in their digital ecosystems.

Finally, antitrust agencies tend to reinforce this subordination of privacy to antitrust law. By and large, it is antitrust agencies—not data privacy enforcers—who are considering this intersection of law.[158] This lopsided attention means much of the theory on how antitrust and data privacy interact is being developed from an antitrust perspective, not a data privacy perspective. The mandate of the antitrust agencies applying those theories is to promote competition, not to protect data privacy (though the FTC is unusual in that it has both mandates).[159] It is thus unsurprising that the primary theory on this overlap of law, privacy-as-quality theory, subsumes data privacy into existing antitrust frameworks as a factor in competition. There has been little attention to impacts in the opposite direction wherein data privacy might influence or change antitrust law. This agency context reinforces competition primacy in theories of intersection between antitrust and privacy law.

Faced with tradeoffs between competition and privacy, the judicial, legislative, and institutional tendency will be to prefer competition—as evidenced in *hiQ v. LinkedIn*, the text of Section 5 of the FTC Act and pending legislation. This developing competition primacy is, at least in part, a function of antitrust treating privacy as a quality-like factor that can be subsumed into existing antitrust frameworks.

To be clear, the problem is not simply that competition is preferred. A preference for competition over privacy may be a legitimate policy choice in some, or even many, contexts. The problem is that this preference is almost entirely unexamined in existing law and policy. Competition is being preferred *without justification* or even contemplation of the real value and identity of data privacy interests. A preference for competition at the cost of data privacy (or vice versa) should be a function of discourse and analysis of the benefits of each, rather than a function of thin antitrust conceptions of privacy, as seems to be the situation now. This Article, by identifying the subordination of privacy to competition in current theory, takes a first step in promoting express dialogue on which interest to prioritize (where they are at odds) and what the justifications are for that primacy.

III. THE CHANGING CHARACTER OF U.S. DATA PRIVACY LAW AND ITS IMPACTS ON ANTITRUST THEORY

After years of growing dissatisfaction and criticism in the digital world, U.S.

158. *See* Part I. B. The Current Theory: Antitrust Understands Privacy as an Element of Product Service or Quality.

159. *See, e.g.*, Statement of FTC Concerning Google/DoubleClick, *supra* note 36, at 2 (finding a lack of jurisdiction to intervene in the transaction based on asserted privacy harm).

data privacy law is in the midst of a revolution.[160] Old models are being harshly interrogated and new paradigms are edging in. This new era will determine the shape of digital privacy for decades to come.[161]

This Part explains the important ways in which data privacy law is changing, then considers what those changes mean for the interaction of privacy with antitrust law. It begins with the origin story of this privacy revolution, summarizing the widespread dissatisfaction with the dominant paradigm of notice and consent-based privacy law. It then examines two of the most significant paradigm shifts underway in U.S. privacy law in response: the emergence of prohibitions in place of notice and consent and the proliferation of privacy rights.

It argues that both changes will produce more variable interactions with antitrust law. Each reflects a growing willingness of data privacy law to question the assumption that data commercialization is beneficial for individuals.[162] Antitrust has, so far, relied on this assumption in its reconciliation with data privacy. As it no longer always holds, we will see a more fragmented landscape of interactions between the two areas of law that demands additional theorization.

A. The Frailties of Notice and Consent

As this Section explains, there is deep and longstanding dissatisfaction with the "notice and consent" model of data protection in U.S. privacy law. As discussed above, this approach to privacy protection requires that companies inform individuals about how their personal information will be collected and used (the "notice"), and then to seek consent from those individuals to the described use. Provided such notice and consent occurs, U.S. data privacy law has, until quite recently, permitted the processing of personal data in ways that are consistent with that notice.[163]

For decades, privacy scholars, policymakers, and consumer advocates have harshly criticized this model of notice and consent for its failure to protect individual's privacy.[164] The literature describes notice and consent on a scale ranging

160. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1690 (2020) ("The modern data industrial complex is facing a tidal wave of public support for a privacy law revolution."); David Doty, *The Privacy Revolution In Digital Is Unstoppable*, FORBES (May 20, 2019, 01:58 PM), https://www.forbes.com/sites/daviddoty/2019/05/20/the-privacy-revolution-in-digital-is-unstoppable/?sh=596212f3d83f [https://perma.cc/E36E-6RDJ] ("[W]e are in a new paradigm . . . .").

161. Hartzog & Richards, *supra* note 160, at 1693 ("[W]e are on the cusp of a set of legal changes that will structure our emergent digital society for decades to come.").

162. The term "data commercialization" is used to mean the business of collecting, analyzing, and then profiting from personal information, particularly in digital services.

163. *See infra* Part III. The Changing Character of U.S. Data Privacy Law and its Impacts on Antitrust Theory.

164. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881–82 (2013).

from, at best, "quaint,"[165] "outdated"[166] and at worst, "broken,"[167] plagued by "fundamental problems"[168] and "in crisis."[169] Perhaps most tellingly, multiple FTC Commissioners—the very enforcers tasked with upholding the federal privacy laws premised on notice and consent—have regularly expressed skepticism over its effectiveness.[170] The current FTC leadership goes even further, labelling notice and choice plainly as "a failure."[171]

There is a rich literature on the array of problems with notice-and-consent privacy law that dates back to at least the 1990s.[172] This Article does not seek to re-summarize this literature in full, which is done well elsewhere.[173] Instead, it highlights the problems with notice and consent by describing two of the most widely recognized critiques: (i) notice and consent is unable to scale meaningfully in

---

165. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY 160 (2016) (describing privacy control, embodied in notice and consent).

166. Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 356 (2022) (describing notice and consent).

167. *Id.* at 361.

168. Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* BIG DATA, PRIVACY AND THE PUBLIC GOOD 45 (Julia Lane, Victoria Stodden, Stefan Bendar & Helen Nissenbaum eds., 2015) (explaining that the implementation of consent models has "fundamental problems").

169. Dennis Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in The Age of Predictive Analytics*, 79 MD. L. REV. 439, 446 (2020).

170. Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable 3 (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf [https://perma.cc/5R6T-PAEP] ("We all agree that consumers don't read privacy policies."); Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, The Near Future Of U.S. Privacy Law at Silicon Flatirons-University of Colorado Law School 7 (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf [https://perma.cc/4XGF-N73W] ("[I]t is time for the reign of notice and consent to end.").

171. Sam Levine, Director, Fed. Trade Comm'n Bureau of Consumer Protection, Remarks at the 2023 Consumer Data Industry Association Law & Industry Conference 3 (Sept. 21, 2023), https://www.ftc.gov/news-events/news/speeches/remarks-bcp-director-samuel-levine-2023-consumer-data-industry-association-law-industry-conference [https://perma.cc/P37J-ALHV] (calling notice and choice "a failure" and noting "more than ever before, leadership of the FTC is stating that plainly").

172. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (privacy notices are often ignored by individuals, written in legalistic language and leave little opportunity for meaningful choice); Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent in Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information (2009) (examining the failures of notice and consent in the context of online advertising, include that data uses are opaque to individuals and privacy policies change often and on short notice); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SEC. & PRIV. 26, 26–30 (2005) (describing how bounded rationality and incomplete information affect privacy-related behavior); Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, *supra* note 164, at 1883-91 (canvasing an array of problems with notice and consent and related literature); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019) (describing the challenges of consent-based privacy protection); Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617 (2021); *cf.* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2013).

173. *See* sources cited at footnote 172.

the digital world, and (ii) there are well-known human pathologies and biases that act as barriers to meaningful notice and consent.

A major critique of notice and consent is that it does not work well at the scale of the modern information economy.[174] The legal approach to notice and consent has remained largely unchanged since the 1970s, but the economy in which it exists has changed dramatically.[175] Thanks to the rise of online connectivity and digital commerce, personal data processing is ubiquitous. Every mouse click, app use, and online page visit now produces personal data that is collected, used, and often sold by digital companies for use in advertising or online services. Our cars, toasters, and even our lightbulbs are connected to the internet, which enables these devices to collect and share digital data.[176] This proliferation of data processing has created an accompanying explosion in the requests for consent.[177] With every connected action, from visiting a webpage to plugging in a new smart toaster, companies purport to offer users a choice of whether to allow the collection and use of their personal data.

The notice and consent paradigm has been labeled privacy "self-management" for precisely this reason—because it leaves privacy choices up to each individual.[178] Yet scholars have long acknowledged that no rational person would actually take the time to read and understand the privacy policies that govern processing of their personal data.[179] By one oft-cited estimate, it would take more than two months to read the privacy policies that an average individual encounters online each year.[180] Even if the rare and diligent consumer, let us call her "Carey Careful," spent this time, privacy policies have become ever-longer and more legalistic, making their text incomprehensible to the average reader. Add to this the problem that privacy policies are not static; companies regularly change the terms of data collection and use.[181] Carey Careful would have to routinely recommit massive amounts of time to actively manage her data privacy.

Further, even if Carey read and understood privacy policies, meaningful consent at scale would still remain elusive. In the digital world, an individual's

---

174. *See, e.g.*, Solove*, supra* note 164 at 1888 (summarizing the problems of scaling up consent in the digital economy).

175. *Id.* at 1881–82.

176. *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 14 (2015) (describing the proliferation of internet connected devices and the massive volumes of data being collected as a result).

177. Solove*, supra* note 164 at 1888.

178. *Id.* at 1882.

179. Acquisti & Grossklags, *supra* note 172 (summarizing empirical and theoretical research on consumer privacy irrationality).

180. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012) (estimating that it would take a consumer seventy-six work days to read the privacy policies encountered in the span of just one year) https://www.theatlantic.com/technology/archive/2012/03/reading-theprivacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851 [https://perma.cc/E2DZ-C4CM]. This figure would likely be much higher now, given the growth in online activity since 2012.

181. Barocas & Nissenbaum, *supra* note 172 (describing privacy policies as "fickle" and "flimsy" given the power and tendency of companies to change their terms).

consent to a single instance of data collection can have significant and highly unpredictable effects when combined with the *other* digital data of that individual and others. While Carey may willingly disclose individual points of "surface" data—for example, saying "yes" to the tracking of her location by one app—it is almost impossible for her to understand or consent to the array of inferences that may be drawn once that data is connected to the rest of her digital data footprint.[182]

For example, a user might willingly consent to each app on their phone tracking their location. But in an unsettling article, the New York Times was able to purchase and cross-reference a wealth of this "anonymized" app data to identify individuals living in New York City, including a 46-year-old math teacher named Lisa Magrin.[183] Using location data collected as often as every two seconds by her smartphone, Lisa was identified based on regular travel from her work to her home, to Weight Watchers, and then to an ex-boyfriend's apartment.[184] While Lisa consented to each individual app tracking her location, she did so without the knowledge that consent could, in aggregate, reveal her identity.

Lisa and Carey provide simple examples. The power of artificial intelligence is being applied to troves of digital data. This dramatically multiplies the ability to cross-reference and draw correlations that are not obvious from individual data points. "Data analytics" or "data mining" refers to the use of increasingly sophisticated artificial intelligence and algorithms to draw inferences from the troves of digital data now being produced by our everyday lives.

Companies are mining digital data to discover unseen connections that inform otherwise unpredictable outcomes in business decisions, from marketing and hiring to credit approvals.[185] For example, data mining reveals that credit card customers who purchase felt foot-pads for their dining chairs are more likely to pay off their next credit card bill than customers who recently purchased chrome skull ornaments for their car.[186] Users of Firefox and Chrome browsers are more likely to remain in a job for a longer period of time than employees who use other browsers.[187] Data mining offers these types of surprising and often valuable correlations to businesses,

---

182. Hirsch, *supra* note 169.

183. Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/UX4E-VWHF].

184. *Id.*

185. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIV. L. 74, 78 (2013) ("[U]sers lack knowledge of potential correlations, they cannot knowingly consent to the use of their data for data mining or Big Data analytics.").

186. Dana Flavelle, *What the Data Crunchers Know About You*, TORONTO STAR (April 23, 2010), https://www.thestar.com/business/tech_news/2010/04/23/what_the_data_crunchers_know_about_you.html [https://perma.cc/8NLQ-SYSC].

187. E.H., *How Might Your Choice of Browser Affect Your Job Prospects? Users of Firefox and Chrome May Stay in Their Jobs for Longe*r, THE ECONOMIST (April 11, 2013), https://www.economist.com/the-economist-explains/2013/04/10/how-might-your-choice-of-browser-affect-your-job-prospects [https://perma.cc/4Q6E-X2XF].

which is why it has become wildly popular.

But the unexpected nature of these correlations tends to defeat both notice and consent. Individuals cannot truly understand what they are disclosing to companies, because of the unpredictability of correlations and inferences that may be drawn once their data is cross-referenced with other data. At the same time, companies cannot robustly disclose the unpredictable insights they will extract and use from that data.[188]

The second major criticism of notice and consent is that human cognitive biases impact individuals' ability to consent in a meaningful way. The literature catalogues a variety of common pathologies that make it difficult for individuals to truly understand the extent and variation of how their data is used in the digital ecosystem. For example, humans have well-documented tendencies to prefer default options in many contexts.[189] This makes it unlikely that users of a digital service will switch to a privacy option different from that initially presented.[190] Companies have long used prechecked boxes to obtain consent to privacy policies, knowing full well that given this cognitive bias, users are unlikely to take the action required to "un-check" to refuse data processing. Humans also tend to over-value present gratification.[191] This makes it more likely that users will choose the immediate reward of access to a needed digital service over the uncertain, long-term impacts that might arise from allowing that service to process our personal data. The list of biases that can undermine meaningful notice and consent goes on, each with a catchy name: the lulling effect (the belief that privacy rights exist merely because legal language is used), the overload effect (the tendency of readers to arbitrarily skim or pick out certain details when presented with large amounts of information—such as a privacy policy), anchoring (the human tendency to latch on to the information presented earliest in time), and more.[192] These biases deeply limit the conscious ability of individuals to choose products and services that are consistent with their expressed privacy preferences.[193] Many of these biases or pathologies are used by companies to design both their digital interfaces and their

188. Hirsch, *supra* note 169, at 459–60 (explaining that because individuals, and the companies using predictive data analysis, "frequently do not know, at the time of collection, the purpose for which they will use a particular piece of data," notice and consent paradigms are undermined); Barocas & Nissenbaum, *supra* note 168, at 60 (providing notice in such contexts can be "challenging, almost by definition, because the value of big data lies in the unexpectedness of the insights that it can reveal"); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 261 (2013) ("[T]o be meaningful, consent must be specific to the purpose (or context). Yet by its very nature, big data analysis seeks surprising correlations and produces results that resist prediction.").

189. *See, e.g.*, JACQUES CRÉMER, YVES-ALEXANDRE DE MONTJOYE & HEIKE SCHWEITZER, EUR. COMM'N, COMPETITION POLICY FOR THE DIGITAL ERA at 50 (Apr. 4, 2019) [hereinafter Crémer Report].

190. *Id.*

191. Calo, *supra* note 172 at 1052–55.

192. For a thoughtful overview of these various biases related to notice and consent in privacy contexts, see *id.*

193. *Id.*

terms of service to nudge consumers in predictable directions online, undermining the presumed significance of notice and consent.

In sum, it is unrealistic to expect individuals to understand privacy policies, and even if they do, human biases make it unfair to expect meaningful decisions about consent in the complexities of the digital data ecosystem. Consumers live in rational ignorance of what happens to their personal data. Ari Ezra Waldman describes modern "consent" to privacy policies as a performative fiction rather than a substantive interaction: companies seek consent using dense privacy policies, and consumers purport to give that consent at every turn, which shields those companies from most liability for how they use —and misuse— personal data.[194]

1. Responding to the Failures of Notice and Consent: Prohibitions and Duties Emerging in U.S. Data Privacy Law

In response to these failures of notice and consent, among other factors, U.S. data privacy law is changing in significant ways. The following sections explore changes at the forefront of data privacy law, and what each means for antitrust theories of data privacy.

Notice and consent privacy laws assume that data processing is permitted and beneficial for individuals, provided those individuals consent to such processing. This assumption has made for easy reconciliation with antitrust law, which proceeds from a similar premise that competition for data-driven services is positive for consumers.[195] This is not specific to data-driven competition; antitrust law assumes all competition is good, provided it is not deceptive or misleading.

At its newest edges, though, parts of data privacy law are challenging this assumption that data-driven competition is positive. Instead of starting from the premise that personal data will be bought and sold, agencies and scholars are asking normative questions about when such commercialization is appropriate or beneficial. The FTC's recent privacy rulemaking is provocatively self-described as a "crack down on harmful commercial surveillance and lax data security."[196] The term "commercial surveillance" is used pejoratively but defined simply as "the business of collecting, analyzing, and profiting from information about people."[197] This encompasses much of the lawful commercial activity in the digital economy. This demonstrates a new concern around the commercial use of personal data *in itself*, rather than any particular practices or harms that occur when data is processed for

194. ARI EZRA WALDMAN, INDUSTRY UNBOUND 6 (2021).

195. *See* supra Part I. C. So Far, So Easy: Shared Assumptions of Markets and Choice between Antitrust and Data Privacy Law.

196. Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/6G5A-SA4R].

197. Trade Regulation Rule on Com. Surveillance and Data Security: A Proposed Rule by the Federal Trade Commission, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022) (to be codified at 16 C.F.R. chpt. 1) [hereinafter Fed. Trade Comm'n ANPR on Com. Surveillance].

profit in certain ways—such as without consent.[198] Leading privacy scholars have similarly pushed for U.S. data privacy law to reevaluate the pro-market assumption from which it proceeds.[199] Hartzog and Richards observe that "data protection regimes seek to permit more ethical surveillance and data processing at the expense of foundational questions about whether that surveillance and processing should be allowed in the first place."[200]

This shift is beginning to manifest at the edges of U.S. data privacy law. Instead of relying almost exclusively on notice and consent, as it has historically, U.S. agencies and lawmakers are increasingly willing to impose substantive prohibitions on entities that process personal information. The phrase "substantive prohibitions" is used here to mean laws or regulations that make certain data practices unlawful. Instead of focusing on whether or not individuals consented to those practices, these new laws decide which conduct is considered socially harmful and prohibit it. This shift in data privacy law is illustrated by the following developments:

Prohibitions on Processing Certain Types of Data. State legislation has begun to prohibit certain data processing as a means to protect the privacy of personal data. The Illinois Biometric Information Privacy Act now prohibits entities from selling, leasing, trading, "or otherwise profit[ing]" from individual's biometric identifiers.[201] Prior to the passage of the Illinois law in 2008, individuals were free to trade in their biometric data and may also have had it traded without their knowing choice.[202] Now, such practices are not permitted.[203] Other states have passed[204] or pending laws[205] that limit the use of biometric data.

These laws recognize that biometric identifiers are uniquely sensitive personal

198. FED. TRADE COMM'N, FACT SHEET ON THE FTC'S COMMERCIAL SURVEILLANCE AND DATA SECURITY RULEMAKING (2022) ("The FTC is concerned that companies monetize surveillance in a wide variety of ways. Companies may use some of the information they collect to provide products and services, but they can also use it to make money.").

199. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 29 (2021) ("The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current form . . . . [T]he mere fact that people make a tradeoff doesn't mean that the tradeoff is fair, legitimate, or justifiable.").

200. Hartzog & Richards, *supra* note 160, at 1693–94.

201. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15(c) (West 2018)

202. *See id.* (observing "limited State law regulating the collection, use, safeguarding, and storage of biometrics" prior to the passage of the Act).

203. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5(e) (West 2018) ("Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.").

204. TEX. BUS. & COM. CODE ANN. § 503.001 (2023); WASH. REV. CODE § 19.375.010-19.375.900 (2023). These Texas and Washington laws limit the use of biometric data, but their obligations are contingent on obtaining notice and consent rather than an actual prohibition as seen in the Illinois Biometric Privacy Act. Similarly, The Children's Online Privacy Protection Act limits the use of some biometric data, like facial recognition, but only by requiring parental consent.

205. Biometric Privacy Act, Assemb. B. A-1362, 2023-2024 Legis. Sess. (N.Y. 2023); An Act to protect personal biometric data, S.D. 2218, 193d Leg. Sess. (Mass. 2023).

information.[206] Biometrics are inherent to each individual and unchanging, such as fingerprints or retinas.[207] As Senator Al Franken noted in his opening statement to the hearing of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law:

> [B]iometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face—unless, I guess, you go to a great deal of trouble.[208]

In another example of limits on data use, Washington state recently passed a law that prohibits certain uses of data for geofencing.[209] Geofencing is the creation of a virtual boundary around a real-world geographic area and is carried out using location data. When a mobile device enters or exits the defined area, geofencing can be used to trigger the sending of online alerts, advertisements, or notifications to that device.[210] Washington's new law prohibits the implementation of a geofence around an entity that provides healthcare services in person, where that technology is used to identify, track, or collect information about individuals seeking health services or to deliver ads or notifications related to their health data or health services.[211] The effect is to create a new limit on certain uses of location-related health data.

Duties of Data Minimization, Best Interests, and Data Loyalty. More general prohibitions on data processing are also appearing in U.S. privacy law and policy in the form of duties or obligations to minimize data collection.

Since 2018, twelve states have passed their first general data privacy laws.[212]

---

206. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5(C) (West 2018) (observing the unique nature of biometric identifiers means that "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions").

207. *Id.* at 14/10 ("biometric identifier") (defining biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" with a further list of specified exceptions).

208. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing on H.R. 112-851 Before the Subcomm. on Priv. Tech. and the L.*, 112 Cong. 1 (2012) (Statement of Sen. Al. Franken).

209. Washington My Health, My Data Act, tit. 19, ch. 44.28, § 1-15, 68th Leg., Reg. Sess. (Wash. 2023).

210. In a high-profile example of this, antiabortion groups have used geofencing of women's health services locations to deliver pro-life advertisements. Byron Tau & Patience Haggin, *Anti-abortion Group Used Cellphone Data to Target Ads to Planned Parenthood Visitors*, WALL ST. J. (May 18, 2023), https://www.wsj.com/articles/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212 [https://perma.cc/FL3K-B3PW].

211. Washington My Health, My Data Act, tit. 19, ch. 44.28, § 10, 68th Leg., Reg. Sess. (Wash. 2023)

212. This number is changing quickly and is stated as of August 2023 here. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2020); Virginia Consumer Data Protection Act, SB 1392 (2021) (amending Code of Virginia, Title 59.1, chapter 52, consisting of sections numbered 59.1-571 through 59.1-581); Colorado Privacy Act of 2021, COL. REV. STAT. § 6-1-1301; The Connecticut Act Concerning Personal Data Privacy and Online Monitoring, CONN. GEN. STAT. §§ 42-515–525 (2022); The Utah Consumer Privacy Act, UTAH CODE ANN. § 13-2-1 (LexisNexis 2022); Indiana Consumer Data Protection Act, S. 5, 2023 Legis., Reg. Sess. (Ind. 2023); Iowa Consumer Data Protection Act, S. 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023); Montana Consumer Data Privacy Act, S. 384, 68th Legis., Reg. Sess. (Mont. 2023); Oregon Consumer Privacy Act, S. 619, 2023 Legis.,

These laws give individuals an array of new rights, discussed below, and impose corresponding duties on corporations and other entities to act to edify those rights. In particular, several laws include duties or obligations to minimize data processing.[213] Entities subject to these laws (often called "data controllers") are required to limit their collection of personal data to what is adequate, relevant, and reasonably necessary for the stated purposes of the collection.[214] Some of the state laws term this a "duty" of data minimization while others frame it as an obligation.[215] Regardless of the specific form, the intended effect is similar: data minimization bars covered entities from collecting and processing, and in California also from retaining,[216] personal information beyond that which is reasonably necessary and proportionate for the disclosed purposes. In effect, these laws limit the ability of companies and other organizations to collect, maintain, and use personal data.[217] Similar obligations to minimize data collection appear as a guiding principle in the European Union's wide-reaching privacy law the General Data Protection Regulation (GDPR).[218] Data minimization is a central focus of a recent, widely supported federal data privacy bill as well.[219]

These duties represent a shift in U.S. legal thinking about the obligations they place on data processors to limit processing. More data collection is not universally assumed to be beneficial. These changes are emergent—their ultimate significance will depend on the robustness of enforcement of state laws and whether this federal law ultimately passes.

More specialized state laws have also been passed, or are being considered, that impose a form of "duty" to consider the best interests of children in the design of online products and services.[220] California passed legislation in 2022 with

---

Reg. Sess. (Or. 2023); Texas Data Privacy and Security Act, H.R. 4, 113th Gen. Assemb. (Tex. 2023); Florida Digital Bill of Rights, S. 262, 2023 Legis., Reg. Sess. (Fla. 2023); Tennessee Information Protection Act, H.R. 1181, S. 0073 (Tenn. 2023); *see also* Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15 (West 2018) (establishing privacy protection of biometric information).

213. The specific obligations vary somewhat by state, but each focuses on data minimization and reasonable use. *See, e.g.*, Virginia Consumer Data Protection Act, VA. CODE ANN., tit. 59.1, ch. 53 § 59.1-578(A)(1) (Va. 2023); Colorado Privacy Act, S. 21-190, 73rd Gen. Assem., Reg. Sess. § 6-1-1308(3) (Colo. 2021); California Consumer Privacy Act, CAL. CIV. CODE § 1798.100 (a)(3) (Cal. 2020); Utah Consumer Privacy Act, S. 227, 2022 Gen. Sess. § 13-61-302 (Utah 2022); Connecticut Data Privacy Act, Public Act No. 22-15, S. 6, 2022 Legis., Reg. Sess. §6 (Conn. 2023).

214. *See id.*

215. *Compare* Colorado Privacy Act, S. 21-190, 73rd Gen. Assem., Reg. Sess. § 6-1-1308(3) (Colo. 2021) ("duty" of data minimization), *and* Virginia Consumer Data Protection Act, VA. CODE ANN., tit 59.1, ch. 53 § 59.1-578(A)(1) (2023) (obligation of data minimization).

216. CAL. CIV. CODE § 1798.100(a)(3) (West 2020).

217. Hartzog & Richards, *supra* note 166, at 365.

218. European Parliament and Council Regulation (EU) 2016/679 of April 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1, Art 1 (c) ("Personal data shall be . . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').") [hereinafter GDPR].

219. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

220. The California Age-Appropriate Design Code Act, CAL. CIV. CODE § 1798.99.28. *See also* Kids

normative statements that businesses "should consider the best interests of children" when designing, developing, and delivering such products and services that use children's data.[221] The legislation supports this statement of what businesses should do with more specific obligations, such as a requirement that default online settings be configured to offer a "high" degree of privacy when provided to children.[222] The law is slated to go into effect in 2024 but is subject to an ongoing constitutional challenge.[223]

While more nascent, U.S. privacy law reform is also paying significant attention to broader duties of "data loyalty." A duty of data loyalty would require companies (or other entities, termed "information fiduciaries") to act in the best interest of the individuals whose personal information is being collected and processed.[224] Specific proposals vary, but duties of data loyalty are modeled on the fiduciary duties that the law imposes on other trusted parties, such as corporate directors, agents, and many professionals.[225] Scholars have long called for the imposition of duties of care and loyalty in data processing.[226] This dialogue has recently matured into a flurry of proposed legislation at the federal and state level.[227] Each of these bills would impose new fiduciary duties of loyalty on entities that process personal information.[228]

Such duties of loyalty, like the other duties and prohibitions discussed here,

---

Online Safety Act, S. 3663, 117th Cong. § 3 (2021) (framed as a duty of care but requiring platforms covered by the law to act in the best interests of a minor that uses the platform's products or services). Similar laws are being proposed in other states and already exist in other leading jurisdictions such as the U.K.

221. *Id.* § 1798.99.29.

222. *Id.* § 1798.99.31(4)(6) (requirement for default privacy settings). This law includes other obligations around assessment of impacts on children from use of their data and use of clear language.

223. NetChoice, LLC v. Bonta, No. 22-CV-08861-BLF, 2023 WL 6135551, at *20 (N.D. Cal. Sept. 18, 2023) (issuing a preliminary injunction enjoining enforcement of The California Age-Appropriate Design Code, based on the plaintiff's demonstrated likelihood of success on claims that the Code would not withstand scrutiny under the free speech clause of the First Amendment). The decision was pending on appeal before the Ninth Circuit as of writing.

224. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE DIGITAL AGE 103 (2004) (proposing fiduciary duties in privacy law; "I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us."); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 966–67 (2021); Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1216 (2016).

225. *See, e.g.*, Richards & Hartzog, *supra* note 224, at 964 (calling for a duty of loyalty in privacy and analogizing to duties imposed by the law on other trust parties); Balkin, *supra* note 224, at 1207-8 (calling for a duty of loyalty would require those fiduciaries to act in the principal's interests as well as a duty of care that would require information fiduciaries to "act competently and diligently" to avoid harm to the interests of the information principal); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 145–46 (2020).

226. *See* Hartzog & Richards, *supra* note 166, at footnote 3 (tracing scholarly calls for a "version" of duties of loyalty in privacy law back more than twenty years).

227. *See, e.g.*, Data Care Act of 2021, S. 919, 117th Cong. (2021); Consumer Online Privacy Rights Act, S. 119, 117th Cong. (2021); New York Privacy Act, S. 6701, 2021 Leg. Reg. Sess. (N.Y. 2021); Massachusetts Information Privacy Act, H.R. 142, 192nd Leg. Reg. Sess. (Ma. 2021); *See also* bills and legislation 220 *infra* at note (focusing on duties specific to children's privacy.

228. *See* bills cited at footnote 227.

would be a significant shift from much of existing U.S. privacy law. Instead of placing the onus on individuals to read notices and consent, such laws would instead place the primary obligations on companies and other entities, who would have duties to act in the interests of those whose personal data they process.

Prohibitions on Misleading Digital Interfaces. In another example of the new willingness of U.S. privacy law to impose prohibitions, Californian data privacy law now bars privacy options that are deliberately or unnecessarily confusing in their design.[229] So-called "dark patterns" are user interfaces designed to exploit the pathologies and biases that plague individuals when they try to manage their privacy.[230]

Consider the interface a consumer might see when they try to turn off online location tracking in an app. The app's interface asks, "Are you sure you want to end personalized app services?" then presents a misleading set of options: a green button on the right reading "no" and a red button on the left reading "yes." This counterintuitive interface is designed to nudge consumers toward mistakenly selecting the right side, green, "good" option, which will allow the app to continue tracking—despite the consumer's intention to end such tracking.[231] The consumer "consented" to data processing inconsistent with their privacy preferences because of the confusing design interface. In addition to the California legislation preventing such practices, the FTC Chair identified these manipulative interfaces as a focus for agency attention in a 2021 report to Congress.[232] Federal legislation has also been proposed to combat such practices.[233]

Agency Rulemaking Emphasizes New, Substantive Prohibitions on Data Practices. Under the Biden administration, the FTC has also shown a new willingness to pursue substantive prohibitions on data practices. For the first time, the agency is seeking to create general regulations to protect data privacy using its rulemaking power related to Section 5 of the FTC Act.[234] In the advance notice of proposed rulemaking, the FTC solicited input on whether it has the authority under Section 5 of the FTC Act to place "a greater set of substantive limits on data

229. The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 999.306 (West 2018).

230. See Part III.A *infra*, The Frailties of Notice and Consent, for a discussion of these pathologies and biases.

231. For a useful typology of several dark patterns used in digital services, see Colin M. Gray et al., *The Dark (Patterns) Side of UX Design* (Proc. 2018 CHI Conf. on Hum. Factors Computing Sys., Paper 534, 2018).

232. FED. TRADE COMM'N, *supra* note 3 (discussing dark patterns); *see also*, Rebecca Kelley Slaughter, FTC Commissioner, Bringing Dark Patterns to Light: An FTC Workshop 1 (Apr. 29, 2021) (introductory comments of FTC Commissioner Rebecca Kelley Slaughter), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf [https://perma.cc/6JTY-U5AL]. Internationally, the U.K. competition and data privacy agencies are closely examining the role of similar "choice architecture" on users' ability to make informed choices about the processing of their personal data. U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO 21 (May 19, 2021).

233. Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. § 3(a)(1) (2019).

234. 15 U.S.C.A. § 57a (West 2011) (Section 18 of the FTC Act authorizes the FTC to promulgate, modify, and repeal trade regulation rules that define with specificity acts or practices that are unfair or deceptive in or affecting commerce within the meaning of Section 5(a)(1) of the FTC Act).

collection" and, if so, what limits may be appropriate.[235] The Chair of the FTC framed this focus on substantive privacy protections as a "[g]rowing recognition of the limits of notice and consent" that dominate existing privacy law.[236]

The FTC has also shifted toward more prohibitions in its privacy remedies. In three recent actions, the agency charged companies with unlawfully sharing the sensitive health data of individuals.[237] Instead of simply ordering the companies to obtain consent before sharing such information, the remedial orders prohibit the companies from using health data for advertising purposes at all.[238] This reflects the shift beyond notice and consent toward prohibitions on the use of data, in response to certain privacy misconduct.

While recent and striking, this agency shift can also be understood as the culmination of decades of FTC enforcement of Section 5 of the FTC Act. Over the last twenty-five years, the agency has brought an ever-expanding array of privacy and data security claims under Section 5.[239] What began as a process-oriented effort to enforce the privacy promises that companies make to consumers has, over time, developed into more substantive protection of the "reasonable expectations" of consumers—regardless of whether or what promises companies make.[240]

Several states are in the process of passing, or have recently passed, regulations that define prohibited practices under new state privacy laws.[241] These rules are the first of their kind and their existence signals a more proscriptive era of privacy law at the state level. For example, California's new privacy legislation bars certain use of sensitive personal information,[242] and the regulations add detail to this

---

235. Fed. Trade Comm'n ANPR on Com. Surveillance, *supra* note 197, § IV(b) Q.21; § IV(d) Q.43; § IV(d) Q.48.

236. FED. TRADE COMM'N, COMM'N FILE NO. R111004, STATEMENT OF CHAIR LINA M. KHAN REGARDING THE COMMERCIAL SURVEILLANCE AND DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING (2022).

237. Complaint, In re BetterHelp, Inc., C-4796, (F.T.C., July 7, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpcomplaintfinal.pdf [https://perma.cc/665M-CC3G]; Complaint, US v. Easy Healthcare Corp., 23-cv-03107 (N.D. Ill. May 17, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf [https://perma.cc/G65Q-784H]; Complaint, US v. GoodRx Holdings, Inc., 23-cv-460 (N.D. Cal. Feb. 1, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf [https://perma.cc/Q4S5-VLF4].

238. Order, United States v. Easy Healthcare Corp., 23-cv-03107 (N.D. Ill. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf [https://perma.cc/F6CK-T95Y]; Order, United States v. GoodRx Holdings, Inc., 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf; Order, In re BetterHelp, Inc., C-4796 (F.T.C., July 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf [https://perma.cc/Q7P5-8V8E]

239. Solove & Hartzog, *supra* note 16, at 661 (observing that "the FTC cases have evolved from enforcing promises to developing more substantive baseline standards that have become nearly independent of the statements made in privacy policies" and tracing this development through specific FTC complaints).

240. *Id.*

241. *See, e.g.*, California Privacy Protection Agency, CAL. CIV. REGS. tit. 11 § 7000-7304 (regulations adopted under California Privacy Rights Act in March 2023).

242. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.121 (West 2020). While

prohibition, including requirements for operationalizing links and requests to prevent such processing.[243]

Taken together, these developments represent a significant, though still emerging, shift in U.S. data privacy law. Notice and consent remains at the core of U.S. privacy law, and by some predictions will always be a part of it.[244] But as criticism of notice and consent reaches a fever pitch, U.S. privacy law is responding with notable change at the edges. In particular, this change includes a move toward more substantive obligations. This novel willingness to impose prohibitions and duties in U.S. data privacy law is a paradigm shift, albeit a partial one. Where once data commercialization and consumer choice prevailed, each of these new laws moves beyond notice and consent to delineate data processing that is prohibited. In doing so, these new laws move beyond efforts to construct "better signage along the road to hell"[245] of notice and consent, toward a new era of more substantive privacy protections in U.S. law.

2. Changing Interactions Between Antitrust Law and Data Privacy: New Variability, Differing Assumptions About Data Commercialization

This shift away from notice and consent is significant for antitrust law. Where once privacy and antitrust law shared an assumption that data-driven competition is positive for consumers, now there lies a more fragmented landscape of interactions.[246] As this Section explains, these new prohibitions and duties split the interactions between antitrust and data privacy into three basic types: (i) the "old" style interactions of notice and consent, wherein both areas of law continue to emphasize consumer choice; (ii) new interactions where privacy law limits or precludes competition, by imposing prohibitions or duties on commercial uses of personal data; and (iii) interactions that are newly murky where privacy law introduces legal standards that differ from that of antitrust law. Existing antitrust theory of privacy lacks the pluralism or nuance to account for this new variability.

Antitrust law assumes that competition, provided it is not deceptive or misleading, is positive for consumers.[247] The legislative scheme of the Sherman Act

---

this is framed as a consumer right to limit use, there are corresponding prohibitions on the business from using the sensitive data once that right is exercised.

243. *See, e.g.*, California Privacy Protection Agency, CAL. CIV. REGS. tit. 11 § 7014 (Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link) and § 7027 (Requests to Limit Use and Disclosure of Sensitive Personal Information).

244. Solove & Schwartz, *supra* note 80, at 1270 ("Although both of us have strongly criticized the notice-and-choice approach, we concluded that moving away from it entirely would be too drastic a paradigm shift for U.S. privacy law.").

245. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 998 (2023).

246. See discussion on choice commonalities in Part I, *infra*, Existing Antitrust Theory: A Unitary Perspective on Data Privacy.

247. Nat'l Soc'y of Pro. Eng'rs v. United States, 435 U.S. 679, 695–96 (1978); F.T.C. v. Sup.

precludes inquiry into whether competition is "good" or "bad"—instead, it assumes that competition improves consumer welfare.[248] Privacy-as-quality theory relies upon this same assumption that competition is good and, relatedly, that consumers will make privacy choices that spur competition between companies to offer better privacy protection.

But the data privacy laws outlined above no longer assume that the commercial use of personal data is necessarily "good." Consider the Illinois Biometric Information Privacy Act, which prohibits trade in biometric information. This legislation, in effect, eliminates any previous competition for the sale of biometric information. Instead of privacy being dependent on choice in the market, that choice is legislated away.

This new future of data privacy law is no longer exclusively about choice in markets. It has become more interventionist in some parts, replacing choice with guardrails or boundaries around the ways in which data may be used or collected. Regulation, not choice, will be the determinant of privacy protection in these spaces.

In fact, many of these new data privacy paradigms are touted precisely because they move the law away from consumer choice.[249] Woodrow Hartzog and Neil Richards argue that the major advantage of a duty of loyalty is that it replaces notice and consent; it "shifts the law's attention from the procedural rules of privacy law that are too easy to manipulate ('Did you hide a vague sentence in the privacy policy? Did the consumer fail to hit the tiny opt-out button?') to the substantive question of what practices go too far." [250] Instead of privacy protection relying on formalistic notions of notice and consent, privacy obligations would stem from the reality of a company's relationships with individual data subjects.[251] This is why the duty of loyalty offers, in their words, "a way out of privacy's consent trap."[252] Dennis Hirsch describes the same shift as a "core feature" of the most significant new scholarly proposals for data privacy law. Each emphasizes "social protection, rather than individual control [in a] shift from a liberalist regulatory approach that seeks to facilitate individual choice, to one that empowers public officials to make choices about which . . . practices are safe for individuals and consistent with social values, and which are not."[253]

Ct. Trial Laws. Ass'n, 493 U.S. 411, 425 (1990) (refusing to consider whether the restraint of trade among criminal defense lawyers served a social good more important than competition: "[t]he social justifications proffered for respondents' restraint of trade . . . do not make it any less unlawful").

248. *Nat'l Soc'y of Pro. Eng'rs*, 435 U.S. at 695–96 ("[T]he statutory policy [of the Sherman Act, the primary federal antitrust law] precludes inquiry into the question [of] whether competition is good or bad.").

249. *See, e.g.*, Woodrow Hartzog & Neil Richards, *We're So Close to Getting Data Loyalty Right*, IAPP (June 14, 2022) (describing proposed federal privacy legislation that contains a duty of loyalty as "a sincere attempt to move beyond the ineffective 'notice and choice'").

250. *See, e.g.*, Hartzog & Richards, *supra* note 166, at 359.

251. *Id.* at 367.

252. *Id.* at 360.

253. Hirsch, *supra* note 169, at 461–62.

Privacy-as-quality theory offers little insight into these new paradigms of data privacy protection. The prohibition or duty will become the determinative force in establishing minimum privacy-protection requirements, in place of the previous, and, at times, unsatisfactory market-driven outcomes. The shared assumption with antitrust—that the law should promote competition and consumer choice—thus disappears. Antitrust law will need to develop new theories to address data privacy when it is not just a factor in competition but rather exists as its own (intersecting) body of law with the distinct goal of ensuring privacy protection rather than just enabling consumer privacy choices.

To be clear, data privacy law has not engaged in a wholesale elimination of choice—there remains a role for privacy choice beyond these legally mandated, minimum privacy protections, as well as pursuant to existing notice and consent-based privacy laws. But these new prohibitions and duties signal that choice will play less of a role than it has in the past, leaving less common ground between the newest types of privacy law and antitrust.

Some of these changes in data privacy law do not bar data-driven competition but instead bring a new murkiness to how antitrust and data privacy law standards will interact. For example, the lodestar of the duties of loyalty appearing across a number of recent state and federal privacy bills is the "best interest" of the data subject. Entities subject to the duty are obligated to act in those best interests. This best interests standard creates the potential for friction with antitrust law—or at least the need for new theories of reconciliation.

Recall that antitrust assumes competition is positive for consumers. But duties of data loyalty are presented as tools to condemn certain competition as negative.[254] The concept of a "duty of data loyalty" was born from a skepticism of corporate profit motives in data-driven industries and the failures of existing privacy law to protect against perceived data exploitation and commodification.[255] Advocates for a duty of data loyalty emphasize that such a duty would prioritize "people over profits," sacrificing competition when it is achieved through "disloyal data practices" that are undesirable for individuals and society.[256] For example, California's new age-appropriate design code states that, in the design of online products services where "a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children *over commercial interests*."[257] This law reflects a new and more broadly emerging sense that commercial uses of data, particularly sensitive health or children's

254. Hartzog & Richards, *Getting Data Loyalty Right*, *supra* note 249, at 4 ("By taking manipulation, betrayal and self-dealing off the table, loyalty duties allow companies to compete on products that are good for their customers, building trust and sustainable, long-term relationships.").

255. *See generally* Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 166, at 362–63 (reflecting skepticism of "corporate profit motives" in industries driven by personal data processing).

256. Hartzog & Richards, *Getting Data Loyalty Right*, *supra* note 249, at 4 ("[I]f the only way a company can make money is through disloyal data practices, then we should celebrate the failure of this business model.").

257. The California Age-Appropriate Design Code Act, CAL. CIV. CODE § 1798.99.29 (b).

data, can and should be limited in exchange for better data privacy protection.

At times, duties of data loyalty may condemn the same conduct as antitrust law. Both would discourage commercial practices that are deceptive or misleading, which can distort competition as well as harm data privacy. But, in order for such duties of data loyalty to add something useful to existing law, they must prohibit conduct beyond deceptive and misleading data practices. Such practices are already prevented by Section 5 of the FTC Act.

This leaves a zone of conduct where a duty of loyalty applies that may or may not also be prohibited by antitrust law. There may be inconsistency in the obligations imposed by antitrust law and those imposed by duties of data loyalty. Consider, for example, an obligation of "loyal data gatekeeping." This specific sub-obligation is envisioned as part of a duty of loyalty by its strongest proponents.[258] It would require that companies subject to the duty act as loyal keepers of control over personal data, limiting (or granting) third party access to individual's data in a manner consistent with the best interests of those individuals.[259] Digital platform operators control the access of innumerable third parties to their platforms. Amazon controls the access of merchants seeking to sell their products on Amazon Marketplace, Apple controls which app developers are permitted to distribute through the Apple app store, and Meta controls which advertisers reach users of its social media services.

Imagine a platform operator who terminates third-party merchants because those merchants are using personal data in a way that is not in best interests of end users. Many of these merchants also compete with the platform operator's own vertically integrated products or services—think of sellers on Amazon Marketplace who sell products in competition with Amazon's own goods. This termination is required by a duty of loyalty. It may also substantially reduce competition between the platform and the sellers for those goods.

The terminations are necessary to uphold the platform's duty of loyal gatekeeping as envisioned for privacy law. But the same action also creates the risk of antitrust claims for violations of antitrust law, such as a refusal to deal. Under Section 2 of the Sherman Act, a dominant firm's refusal to engage in business transactions with rivals may be unlawful if it serves to maintain or create a monopoly.[260] While duties to deal with rivals are narrow in antitrust law, such claims are more likely to succeed when there is a prior profitable relationship between the plaintiff and defendant,[261] as in this example. Whether or not those antitrust claims

258. Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 166, at 380 (describing a duty of loyal gatekeeping).

259. *Id.*

260. Verizon Commc'ns Inc. v. Law Offs. of Curtis V. Trinko, L.L.P., 540 U.S. 398, 408 (2004) ("Under certain circumstances, a refusal to cooperate with rivals can constitute anticompetitive conduct and violate § 2.").

261. Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585 (1985) (finding a Section 2 violation based on a refusal to deal where there is a prior profitable business relationship between the plaintiff and defendant).

ultimately succeed, the platform operator finds itself caught between its fiduciary duties in privacy and antitrust law. This is not an argument against fiduciary duties in data privacy law. Rather, it is a recognition that as privacy law increasingly turns to such duties, this will give rise to new interactions and complexities where it meets antitrust law.

This privacy friction will be exacerbated by antitrust-like bills that seek to prohibit "self-preferencing" in the United States, and which have already been passed in the European Union. These laws require digital platforms to treat third parties similarly to the platform's own vertically-integrated services.[262] In practice, that means platform operators will have to allow certain third parties to interoperate with their services and to access the user data available on those services. The goal of such laws is to promote competition. It is not clear whether the personal data-driven competition that these laws seek to promote would be in the "best interests" of users from a privacy perspective. New conceptions of data privacy, like a duty of loyalty, may thus lead to antitrust claims against companies or even violations of future statutory obligations not to self-preference. There is no existing antitrust theory to address these interactions.

Finally, there will be a third type of privacy law/antitrust interaction where older-style notice and consent privacy laws persist. The changes above demonstrate a definite shift away from notice and consent, but choice-based privacy law is far from gone. Notice and consent remain a touchstone of many data privacy laws in the United States. While the terms "old" or "older" privacy law are used to describe notice and consent paradigms, even some of the new data privacy laws described above can be cast as redoubling efforts to ensure meaningful consent. For example, the prohibition on dark patterns helps individuals to receive fair and clear options so that they can exercise their true privacy preferences. This means that privacy-as-quality theory will remain relevant to the antitrust analysis where privacy law continues to emphasize consumer choice through notice and consent. In these areas of law, the shared assumption remains that competition and consumer choice are paramount and beneficial. The forces of competition will still be expected to drive increased data privacy, and, as such, privacy-as-quality theory continues to be relevant and applicable to these choice-based interactions.

Continuing the example of new prohibitions on dark patterns in privacy law, antitrust does not condone competition based on misleading conduct. Dark patterns can often be misleading.[263] If a company uses dark patterns to unlawfully reduce competition, such as to maintain a monopoly, then both antitrust law and the new California dark pattern legislation would likely condemn the practice. In these areas of data privacy law where choice continues to be important, antitrust enforcement will often be consistent with privacy law.

---

262. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021); American Innovation and Choice Online Act, H.R. 3816, 117th Cong. (2021).

263. FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT (2022) (observing that "dark patterns are covert or otherwise deceptive, [and] many consumers don't realize they are being manipulated or misled" by them).

Across these interactions of antitrust with new and older paradigms of data privacy law, what emerges is a sense of unprecedented variability. As this Section shows, where there was once a shared emphasis on consumer choice, now there is more. In some areas, privacy-as-quality theory will remain relevant to the antitrust analysis. In others, antitrust will require new thinking, to address data privacy law that no longer relies on consumer choice, or that is based on standards like "best interests" that are potentially distinct from antitrust measures of consumer welfare. Antitrust theory has not yet grappled with this shift in privacy law beyond notice and consent, and has only recently come around to thinking about data privacy much at all.[264]

B. The Rise of Rights in U.S. Data Privacy Law

There is a second profound change occurring in U.S. data privacy law—the proliferation of privacy rights. As this Section explains, this new rights identity will also bring greater variety to the interactions between data privacy and antitrust law. While less obvious than for the prohibitions discussed above, this rights identity also challenges the assumption that personal data should be available for sale.

In some sense, rights have long been a part of U.S. privacy law. In 1890, Samuel Warren and Louis Brandeis first conceived of privacy as "the right to be let alone."[265] The 1973 Fair Information Practices ("FIPs," or sometimes "FIPPs") are often identified as the root of U.S. data privacy law.[266] The FIPPs are framed in relation to the "rights of citizens."[267] From the 1970s onward, rights have also appeared occasionally in sectoral data privacy law statutes, such as the rights to opt out of information sharing in the Gramm-Leach-Bliley Act,[268] the Fair Credit Reporting Act,[269] and Health Insurance Portability and Accountability Act.[270]

However, over the last five years U.S. privacy law has seen an unprecedented proliferation of data privacy rights.[271] This new momentum in privacy rights is most visible at the state level. Beginning with California in 2018, twelve states have now passed their first-ever broad, data privacy protection statutes.[272] These state laws

---

264. See discussion at Part I on the current theory of antitrust law and data privacy.

265. Warren & Brandeis, *supra* note 11, at 195.

266. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41–42 (1973) (articulating the FIPS).

267. *Id.*

268. The Gramm-Leach-Bliley Act requires that consumers be given the right to opt out of a financial institution's disclosure of nonpublic personal information about them to a nonaffiliated third party unless an exception applies under the Act. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in relevant part primarily at 15 U.S.C. §§ 6801–6809 (2021)).

269. Affiliate Marketing Rule, 72 Fed. Reg. 61424 (Oct. 30, 2007) (discussing the right introduced by the Fair and Accurate Credit Transactions Act of 2003 amendments to the FCRA (s. 264)).

270. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in sections of 18, 26, 29, and 42 USC).

271. *See* Solove, *supra* note 245, at 979–84 (observing the rise of privacy rights in U.S. state law and GDPR).

272. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2020); Virginia Consumer Data Protection Act, SB 1392 (2021) (amending Code of Virginia, Title 59.1, chapter

establish a panoply of different, groundbreaking privacy rights that have never before existed in U.S. law.[273] This wave of rights-driven privacy legislation is poised to expand, as several other states actively consider similar laws.[274]

Where there were once just occasional rights of opt out or correction of data, these new state laws lay out an expansive menu of rights. The specifics vary somewhat by state statute, but all are modeled on the leading California legislation. The California law grants individuals numerous rights that are enforceable against a business that collects their personal information, including the following:[275]

- Right to demand the deletion of personal information, with some exceptions;[276]
- Right to limit the use and disclosure of sensitive personal information;[277]
- Right to opt out of the sale or sharing of personal information;[278]
- Right to request disclosure of the categories of personal information being collected or sold by a business, the sources of the collection, and its purpose;[279]

52, consisting of sections numbered 59.1-571 through 59.1-581); Colorado Privacy Act of 2021, COL. REV. STAT. § 6-1-1301; The Connecticut Act Concerning Personal Data Privacy and Online Monitoring, CONN. GEN. STAT. § x-x (2022); The Utah Consumer Privacy Act, UTAH CODE ANN. § 13-2-1 (LexisNexis 2022); Indiana Consumer Data Protection Act, S. 5, 2023 Legis., Reg. Sess. (Ind. 2023); Iowa Consumer Data Protection Act, S. 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023); Montana Consumer Data Privacy Act, S. 384, 68th Legis., Reg. Sess. (Mont. 2023); Oregon Consumer Privacy Act, S. 619, 2023 Legis., Reg. Sess. (Or. 2023); Texas Data Privacy and Security Act, H.R. 4, 113th Gen. Assemb. (Tex. 2023); Florida Digital Bill of Rights, S. 262, 2023 Legis., Reg. Sess. (Fla. 2023); Tennessee Information Protection Act, H.R. 1181, S.B. 0073 (Tenn. 2023); *see also* Biometric Information Privacy Act, 740 Ill. COMP. STAT. ANN. 14/15 (West 2018) (establishing privacy protection of biometric information).

273. Press Release, California Department of Justice, Attorney General Bonta Announces First-Year Enforcement Update on the California Consumer Privacy Act, Launches New Online Tool for Consumers to Notify Businesses of Potential Violations (July 19, 2021), https://oag.ca.gov/news/pres s-releases/attorney-general-bonta-announces-first-year-enforcement-update-california [https://perma.cc/R94R-LNP8].

274. *See, e.g.*, H.R. 4514, 192nd Leg. Reg. Sess. (Ma. 2022), S. 2687, 192nd Leg. Reg. Sess. (Ma. 2022); H.R. 5989, 101st Leg. Reg. Sess. (Mi. 2022); S. 332, 202th Leg. Reg. Sess. (N.J. 2022); H.R. 376, 134th Leg. Reg. Sess. (Oh. 2022); H.R. 2257, 2021 Leg. Reg. Sess. (Pa. 2022).

275. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.105-125 (West 2020); other rights less relevant to this discussion. The California Consumer Privacy Act afforded individuals rights to know what information businesses have about them, to data portability, and to data deletion. This set of rights expanded with the 2020 California Privacy Rights Act, which amended the CCPA to add rights to correction, the right to limit the use and disclosure of sensitive personal data, and rights to nondiscrimination against consumers on the basis of their exercise of privacy rights.

276. CAL. CIV. CODE § 1798.105 (West 2020); *see also* COLO. REV. STAT. § 6-1-1302(1)(c)(ii)(a) (2021); 2023 Conn. Pub. Acts No. 22-15, § 4; VA. CODE ANN. § 59.1-577 (2022); UTAH CODE ANN. § 13-61-201 (2022).

277. CAL. CIV. CODE § 1798.121 (West 2020).

278. CAL. CIV. CODE § 1798.120 (West 2020); *see also* COLO. REV. STAT. § 6-1-1302(1)(c)(ii)(a) (2021); 2023 Conn. Pub. Acts No. 22-15, § 4; VA. CODE ANN. § 59.1-577 (2022); UTAH CODE ANN. § 13-61-201 (2022).

279. CAL. CIV. CODE § 1798.110 (West 2020); *see also* COLO. REV. STAT. § 6-1-1302(1)(c)(ii)(a) (2021); 2023 Conn. Pub. Acts No. 22-15, § 6; VA. CODE ANN. § 59.1-578 (2022); UTAH CODE ANN.

- Right to data access, meaning an individual has the right to know what categories or specific pieces of personal information a business has collected;[280]
- Right to data correction, where a business has inaccurate personal information about an individual;[281] and
- Right to data portability, meaning the right to obtain data in a readily usable format that enables the individual to transmit it to another entity.[282]

This rights identity is appearing in federal data privacy dialogues as well. Past administrations have proposed a consumer privacy bill of rights.[283] President Biden has expressed support for enshrining data privacy rights in law.[284] Federal bills premised on privacy rights have been proposed at a frenzied rate in recent years,[285] with twenty-four data privacy bills introduced in the 117th Congress.[286] One of these bills, the American Data Privacy and Protection Act, received unprecedented bipartisan and bicameral support.[287] This legislation billed itself as, first and foremost, "provid[ing] consumers with foundational data privacy rights."[288]

---

§ 13-61-302 (2022).

280. CAL. CIV. CODE § 1798.110 (West 2020); *see also* COLO. REV. STAT. § 6-1-1302(1)(c)(ii)(a) (2021); 2023 Conn. Pub. Acts No. 22-15, § 6; VA. CODE ANN. § 59.1-578 (2022); UTAH CODE ANN. § 13-61-302 (2022).

281. CAL. CIV. CODE § 1798.106 (West 2020); *see also* COLO. REV. STAT. § 6-1-1302(1)(c)(ii)(a) (2021); 2023 Conn. Pub. Acts No. 22-15, § 4; VA. CODE ANN. § 59.1-577 (2022).

282. CAL. CIV. CODE § 1798.130 (West 2020) (requiring disclosure of personal information in compliance with other rights "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance"). This is read as, in effect, a right to data portability; *see also* GDPR, *supra* note 218, at art. 20 (right to data portability).

283. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 9–22 (Feb. 2012), https://www.hsdl.org/?abstract&did=700959 [https://perma.cc/3FPV-KTDL] (proposing a "Consumer Privacy Bill of Rights").

284. Editorial Board, *Joe Biden*, N.Y. TIMES (Jan. 17, 2020), https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html [https://perma.cc/V6C9-UDQA] (now President Joe Biden commenting that the United States should be "setting standards not unlike the Europeans are doing relative to privacy").

285. *See, e.g.*, Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (making it unlawful for any entity that "collects or otherwise obtains personal information" to violate privacy rights enumerated in the bill); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020) (providing privacy protections on any data that identifies or is linked to a specific person); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (codifying privacy rights and creating standards for the collection, use, sharing, and protection of consumer data); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2nd Sess. 2022).

286. Müge Fazlioglu, *Privacy Bills in the 117th Congress*, INT'L ASS'N FOR PRIV. PRO., (Aug. 24, 2021), https://iapp.org/news/a/privacy-bills-in-the-117th-congress/ [https://perma.cc/GV3K-7FDJ] (counting bills as one if there is a counterpart in the other Chamber of Congress).

287. H.R. 8152, 117th Cong. (2022). At the time of writing the bill was expected to be reintroduced in a similar form in the 188th Congress.

288. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2nd Sess. 2022), preamble.

1. Changing Interactions with Antitrust Law: A Variety of Data Privacy Rights and Evolving Assumptions About Data Commercialization

This move toward a rights-like identity in U.S. data privacy is significant for antitrust law. Like the prohibitions discussed in the prior Section, these data privacy rights bring new variability to privacy interactions with antitrust law. These rights also reflect a shift away from the previously shared assumption with antitrust that the commercialization of personal data is uniformly positive for consumers.

The proliferation of privacy rights will bring new heterogeneity to the ways in which antitrust and privacy law interact. This is in part because privacy law is not evolving into one unitary right, but rather a constellation of various types of rights. Modern state data privacy laws embody a growing collection of rights from data portability, correction, and deletion to transparency of processing and minimization of data collection, as described above. Some newer proposals include rights related to automated decision-making, such as a right to understand how such decisions are made.[289]

Existing antitrust theory misses the variable interactions these new rights bring about, because it synonymizes privacy with quality-based competition. Under privacy-as-quality theory, more competition is assumed to produce better privacy protection. Under notice and consent privacy laws, antitrust enforcers and policymakers were able to assume this complementarity, and they have.[290] The same complementarity cannot be assumed for all of the emerging privacy rights, because those rights vary in their substance. Some rights are likely to prove complementary with the goals of antitrust law and competition policy, while others are likely to be in tension.

Data portability rights are perhaps the most likely to remain complementary with the goals of antitrust law. At the U.S. state level and around the world, data privacy and data protection laws are granting individuals the right to copy, move, or transfer their data from one online service provider to another.[291] Such "data

---

289. *See, e.g.*, White House, Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights* (October 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights [https://perma.cc/24YN-U2ZE] (proposing a right to an explanation of automated decision-making).

290. *See*, Part I.C. So Far, So Easy: Shared Assumptions of Markets and Choice between Antitrust and Data Privacy.

291. *See, e.g.*, GDPR, *supra* note 218, at art. 20 (right to data portability for personal data); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.130(a)(3)(B)(iii) (requiring that businesses provide information obtained from consumers in a format that is structured, commonly used, and machine-readable, to the extent technically feasible that may be transmitted to another entity at the consumer's request), and § 1798.100(d) (requiring businesses to provide personal information to consumers who made a verifiable request in a portable format if provided electronically and, if "technically feasible," in a "useable format that allows the consumer to transmit this information to another entity without hindrance"); Press Release, Austl. Competition & Consumer Comm'n, ACCC Welcomes Consumer Data Right (May 9, 2018) (in May 2018, the Australian government adopted a Consumer Data Right that entitles individuals to access their data and have it transferred, in certain sectors); Personal Data Protection Act (amendment), (Nov. 2, 2020) (Sing.) (passing amendments to the Personal Data Protection Act 2012 (PDPA) to introduces new data portability rights); Personal Data Protection Comm'n of Singapore & Competition and Consumer Comm'n of Singapore, Discussion Paper on Data Portability 6–9 (Feb. 25, 2019) (noting that several jurisdictions, such as Australia, the European Union, India, Japan, Philippines, New Zealand, the U.K., and certain U.S. states have either implemented or are

portability" rights, or "data mobility" rights, empower individuals to request that certain categories of their personal data be made available in a format that enables the data to be transferred from one service provider to another. Though sometimes analogized to the transfer of a phone number to a new phone service provider, modern data portability rights are more complex and can enable more extensive movement of data.[292]

Antitrust authorities cast data portability rights as positive for competition.[293] Because these rights provide individuals with the power to move their personal data from one service to another, the FTC explains that "[d]ata portability may . . . promote competition by allowing new entrants to access data they otherwise would not have, enabling the growth of competing platforms and services."[294] Where personal data was once kept exclusively by a single company, data portability rights seek to free it. The thinking is that data portability rights will enable competition by making it easier and more likely that consumers will switch to new digital services.[295] Without such portability, individuals may be hesitant to try a different service because doing so means leaving behind their digital data on the old service. A switch in social media services means old pictures, messages, and contacts disappear if the user cannot bring this data—so users stay with their existing providers. Portability enables this data to be transported over to new services. The antitrust expectation is that this data mobility will make it easier for new entrants to the market to win over users from incumbent firms, enabling new competition.[296]

---

considering introducing the right to data portability in their domestic laws).

292. Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and other Considerations*, 6 GEO. L. TECH. REV. 57, 6-67 (2022) (canvassing terminology used to describe data portability and related but often broader concepts of data sharing and transfers.)

293. Press Release, Fed. Trade Comm'n, FTC Announces September 22 Workshop on Data Portability (Mar. 31, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/ftc-announces-september-22-workshop-data-portability [https://perma.cc/9MA7-D8Z3] ("Data portability may also promote competition by allowing new entrants to access data they otherwise would not have, enabling the growth of competing platforms and services."); Joaquín Almunia, Vice President of the European Comm'n Responsible for Competition Policy European Comm'n, Remarks at the Privacy Platform Event: Competition and Privacy in Markets of Data (Nov. 26, 2012), http://europa.eu/rapid/press-rel ease_SPEECH-12-860_en.htm [https://perma.cc/G882-32E6] ("[P]ortability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them.").

294. Press Release, Fed. Trade Comm'n, FTC Announces September 22 Workshop on Data Portability (Mar. 31, 2020).

295. *But see* discussion of the limits of data portability rights in promoting competition. ERIKA DOUGLAS, DIGITAL CROSSROADS: THE INTERSECTION OF COMPETITION LAW AND DATA PRIVACY, GLOBAL PRIVACY ASSEMBLY, (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737 [https://perma.cc/D7TS-8UTP].

296. This competition argument contains an unstated assumption, often made by antitrust authorities, that data portability rights will result in consumers moving their data from (often large) incumbents to new firms in the market. However, the directionality of this movement could also be the other way, with consumers taking advantage of the ability to move from smaller upstarts to larger, more established firms. This is made more likely because many digital services are characterized by network effects, which occur where the greater the number of users of a service, the more value the service has to each user. The impact of such effects is that users are likely to favor a larger incumbent

However, other types of data privacy rights are more likely to be in tension with competition. The recently passed state privacy laws all include rights of data deletion that enable consumers to request that a business delete their information.[297] California also includes the right of consumers to opt out of the sale or sharing of data[298] and, separately, to limit the use and disclosure of sensitive personal data.[299] Like the data minimization duties discussed above, these rights seek to limit the processing of personal information as a way to protect privacy.

Antitrust is increasingly focused on the opposite: data proliferation and access to restore competition in online services. There is robust agency, policy, and legislative dialogue on how to create more data access and flow. This push for "data democratization" from Congress and the FTC includes policy efforts to expand data access through changes in antitrust law and enforcement,[300] litigation against large online platforms challenging their exclusion of competitors from online data,[301] and legislative proposals that would mandate interoperability or data sharing obligations for certain digital platforms.[302] Examples include the American Innovation and Choice Online Act, which, as discussed above, would require large digital platforms to treat third parties similarly to the platform's own vertically integrated services.[303] This means third parties will have similar access to personal data that is held by the platform, even if those third parties do not have a direct relationship with the

---

firm with more (other) users. *See, e.g.*, *Crémer Report*, *supra* note 189, at 82–83 (noting some scholars have expressed concern that data portability would diminish competition from small firms and startups but noting that the anticompetitive potential of data portability rights under GDPR "seems to be limited").

297. *See supra* sources cited at footnote 276.

298. The California Consumer Privacy Act of 2018, CAL. CIV. CODE §1798.120 ("A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information.").

299. CAL. CIV. CODE §1798.121.

300. STAFF OF S. COMM. ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REP. AND RECOMMENDATIONS (2020), https://democrats-judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf [https://perma.cc/GZ9A-UCBF] [hereinafter HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS].

301. *See* Complaint, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020) (challenging agreements that require Google search default and presets on mobile devices and other search access points, foreclosing competitor access to that search data).

302. See discussion above on Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of H.R. 3849, 117th Cong. (2021–2022) § 4 (requiring platforms covered by the law to maintain and facilitate interoperability with competing businesses), https://www.congress.gov/bill/117th-congress/house-bill/3849 [https://perma.cc/WT7L-788H]; American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/2992 [https://perma.cc/2TP3-NFYB]; HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 300, at 384-87 (recommending promotion of interoperability and portability to encourage data-driven competition). Similar legislation has already been passed in the European Union. Digital Markets Act, art. 6(9) and 6(10) (both requiring "effective" data portability that includes "continuous and real-time access") and art. 6(11) (requiring that third-party search engines be provided with fair, reasonable, and nondiscriminatory access to certain search data generated by end users and held by the "gatekeeper" platform).

303. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021–2022).

individual whose data they access.

From an antitrust perspective, what matters is not the personal nature of the data being accessed. Antitrust is focused only on whether access to that data would improve competition. But data privacy law is focused almost entirely on the personal nature of the data, seeking to control access to and processing of data because it is *personal* data. This different emphasis can create policy tension, and potentially even conflicts in law, between antitrust efforts to promote data-driven competition and the new data minimization and deletion duties in data privacy law. Collectively, these new privacy rights and duties are likely to make that same data less available to drive digital competition. Personal data is often analyzed and sold to fuel digital services, from ads to apps. Where there is less data available because it was deleted or consumers blocked its sale or it cannot be used because it is sensitive, that reduces the use of such data to drive competition among digital services. These new limits may well be a positive development for privacy, but they can have negative follow-on effects on competition.

Looking deeper, this variability in rights interactions derives from changing assumptions at the edges of U.S. data privacy law. While less obvious than the prohibitions and duties discussed above, the rise of privacy rights also suggests a new skepticism toward the commercialization of personal data.

Antitrust law assumes that competition in data-driven goods and services benefits consumers. It pursues such competition through laws and enforcement that often emphasize access to and the proliferation of data, including personally identifiable information. For antitrust law, personal data is just another locus for competition in the market.

In contrast, the newest U.S. state privacy rights are rooted in European dignitary conceptions of privacy,[304] which are more resistant to the starting assumption that personal data is available to be bought and sold. This connection to data commercialization is best understood by tracing the origins of the new U.S. privacy rights back to European data protection law. In what has been labelled the "Brussel's Effect," powerful European conceptions of privacy are driving the recognition of new privacy rights in U.S. state laws and around the world.[305] State data privacy laws borrow heavily from, and are regularly compared to the GDPR, the European Union's wide-reaching privacy law.[306] While not identical to the

304. *See infra* text accompanying footnotes 308-316.

305. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 19–22 (2012) (discussing the Europeanization of global regulatory standards, including in data privacy and antitrust law); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 166 (2017) (the shared technological context of American internet platforms "acts as a force for convergence" of privacy law and norms); *but see* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 371 (2019) ("GDPR's core principles are rapidly evolving into a *de facto* globalized data protection standard," and adding that, on closer examination, there has been a bilateral transatlantic privacy convergence rather than a unidirectional EU exportation of standards).

306. GDPR, *supra* note 218, at art. 1. Compare definitions of "controller" and "processor" in GDPR 2016 O.J. (L 119) to definitions of the same terms in the Connecticut, Utah, Colorado, and

GDPR, the law's influence on U.S. state legislation is clear from both the similarity of many of the rights and the close timing of their promulgation. The GDPR came into effect in 2018,[307] and state laws began to proliferate around the same time.

This European influence imports with it more skepticism of data commercialization in U.S. law. While U.S. privacy law has its roots in consumer protection, European law recognizes data privacy and data protection as constitutionally-based rights.[308] Privacy has a dignitary status, analogous to a natural right that extends from the moral rights of individuals to self-determination and dignity.[309] Privacy, as a dignitary right, is inalienable.[310] This difference is clear from the starting point of data privacy law in each jurisdiction. The GDPR prohibits the processing of personal data unless certain lawful grounds for such processing are established.[311] In contrast, U.S. data privacy law has long assumed the opposite: that personal data is free to be processed unless the law expressly prohibits that processing.[312]

Under this EU paradigm, it is not a particular use or sale of data that violates but rather the data extraction itself that may be objectionable as an invasion of self.[313] For example, the process of algorithmic decision-making turns individuals into patterns, categories, and machine-readable data, then subjects those same individuals to decisions and governance based on a bits-and-bytes version of themselves.[314] The GDPR responds to this invasion into data subject's autonomy and personal identity by limiting algorithmic decision-making.[315] It confers on individuals the right not to be subject to "a decision based solely on automated processing," with some exceptions.[316]

Over the last decade or more, U.S. privacy scholars have begun to describe privacy in similar terms of dignity and sovereignty. Most notably, Anita Allen objects to the idea of individuals bargaining away or waiving their privacy rights, at least in some core areas, on grounds that privacy is a fundamental right that belongs

---

Virginia data privacy statutes.

307. GDPR, *supra* note 218.

308. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, 397 arts. 7-8 (describing a fundamental right to "the protection of personal data"); GDPR, *supra* note 218 (protecting the privacy of "natural persons with regard to the processing of personal data and the free movement of such data").

309. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) at 397 arts. 7–8.

310. *The EU General Data Protection Regulation*, HUMAN RTS. WATCH (June 6, 2018, 5:00 AM), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/8Y52-LJMX].

311. GDPR, *supra* note 218, at art. 6 (processing lawful only based on the listed grounds).

312. *See, e.g.*, Giovanni Buttarelli, EDPS, Opening Speech at the Youth and Leaders' Summit (Jan. 21, 2019) (observing the distinction that in the United States "in the name of free markets, data is another locus for competition between companies and consumers" whereas in Europe "according to the European Convention on Human Rights and the Charter of Fundamental Rights of the EU, data doesn't belong to anyone but privacy is something inalienable and personal data is something to be treated with respect").

313. *See id.*

314. Salomé Viljoen, *A Relational Theory for Data Governance*, 131 YALE L. J. 573, 624 (2021) (summarizing invasions of dignity and autonomy theorized to result from algorithmic decision-making).

315. *Id.*

316. GDPR, *supra* note 218, at art. 22.

to the core of human dignity.[317] Arguing against "surveillance capitalism" as an invasion of dignitary interests that intertwine data privacy with self, Shoshana Zuboff describes what is at stake in privacy as "the human expectation of sovereignty over one's own life and authorship of one's own experience."[318]

While U.S. data privacy rights have not reached a European-like status, this dialogue is beginning to echo into American data privacy laws. For example, proposed U.S. state[319] and federal laws now seek to place limits on algorithmic decision-making.[320] New state laws also reveal less permissive approaches to alienability of personal data than in the past.[321] The newest federal proposals for U.S. law are more resistant to the easy waiver of rights. The leading proposal for federal privacy legislation, as mentioned above, is framed primarily in terms of individual rights. It includes a provision that hints at greater inalienability: a covered entity *cannot* require that individuals waive obligations to comply with that same privacy law in order to gain access to a product or service.[322] In other words, access to products or services may not be conditioned on a relinquishment of the privacy rights granted by the statute.

This privacy-as-right identity is particularly ill-suited to treatment under antitrust theory of privacy-as-quality. Recall that antitrust treats privacy like any number of other quality parameters, all of which are equal to price in economic terms.[323] Antitrust conceives of individuals as "paying" for services with their

317. ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 156–72 (2011).

318. SHOSHANA ZUBOFF, AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 521 (2019).

319. Stop Discrimination by Algorithms Act of 2021, Washington D.C. Council Bill 240558 (2021), https://legiscan.com/DC/research/B24-0558 [https://perma.cc/26CJ-WA4E].

320. Algorithmic Accountability Act of 2019, S. 1108, 116th Cong. (1st Sess. 2019); The Algorithmic Justice and Online Platform Transparency Act, S.1896, 117th Cong. § 6 (1st Sess. 2021) (prohibiting algorithmic processes on online platforms that discriminate on the basis of race, age, gender, ability, and other protected characteristics); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (1st Sess. 2019) (proposing new requirements for businesses that use algorithmic decision-making to process data). While the U.S. law seeks to combat discrimination in algorithm-driven decisions, the EU law goes further by conferring the right not to be subject to an automated decision—without regard to whether that decision was discriminatory. Note that in the United States there has also been a wide array of more specific legislation focused on facial recognition use by law enforcement. Given the criminal law context these proposed laws, although significant, are left aside for the purposes of this privacy discussion.

321. *See, e.g.*, sources cited at footnote 278 (state law controls over the sale of personally identifiable information).

322. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 104(a) (2nd Sess. 2022) ("Conditional Service Or Pricing Prohibited—A covered entity shall not deny or condition or effectively condition the provision of a service or product to an individual based on the individual's agreement to waive (or refusal to waive) any requirements under this Act or any regulations promulgated under this Act or terminate a service or otherwise refuse to provide a service or product to an individual as a consequence of the individual's refusal to provide such a waiver" with some specified exceptions).

323. *See, e.g.*, Noah Joshua Phillips, Comm'r, Fed. Trade Comm'n, Prepared Remarks at The Center for Internet and Society Stanford Law School: Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy at 3 (Jan. 30, 2020), https://www.ftc.gov/system/files/documents/public_statements/1565039/phillips_-_stanford_speech_10-30-20.pdf [https://perma.cc/AR2D-GZFH] ("Privacy can be evaluated as a qualitative parameter of competition, like any number of nonprice

personal information.[324] Lower levels of privacy—such as more invasive personal data collection, greater loads of targeted advertising, or fewer settings that offer end users options to limit the collection or use of their data—are all conceived of as a higher privacy-adjusted price. This theory remains broadly consistent with the older paradigms of privacy law styled on notice and consent.

But the dignitary identity of European privacy rights, particularly their inalienable nature, finds greater conceptual tension with the antitrust treatment of privacy as price-equivalent. As the former head of the European data protection agency explains, while personal data has value, "even if some people treat personal data as commodity, under EU law it cannot be a commodity. . . . You cannot monetize and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction."[325] Price-equivalent treatment of privacy rights collapses a dignitary interest, intertwined with sovereignty over one's own life and experience, into quantified terms that thoroughly fail to account for its significance.

As the U.S. adopts certain European-style data privacy rights, it will face a similar challenge of paradigm incompatibility with antitrust law. Interactions with new data privacy rights are not explained by an antitrust theory of privacy as quality, for the very reason that theory has worked in the past: it subsumes privacy into market-based frameworks of antitrust law. Even if some U.S. rights continue to be waivable in exchange for access to services or products, this bounded commerciality is not the same as rights being influenced upward or downward in their quality by competition. New state data privacy law confers rights with meaning and identity that are independent from their effects on competition in a market. Their strength is not primarily influenced upward or downward by how companies treat these rights; rather, the legislation itself (and their subsequent treatment in litigation) imbues these privacy rights with their strength. Privacy-as-quality theory cannot account for the relevance of data privacy rights because these rights are not merely a factor in competition, or a function of market forces, but something more in their legal identity. From this perspective, a theory of privacy-as-quality is not only insufficient because of its quantification of dignitary interest, but also because it is logically inapplicable in conducting related antitrust analysis.

Despite the new complexity these privacy rights bring to U.S. law, antitrust never speaks of privacy in terms of rights. Scholarship, agency, and policy dialogues have yet to address the antitrust implications of the emergent state rights or

---

dimensions of output; but competition law is not designed to protect privacy.").

324. *See, e.g.*, Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 64 (2019) ("[L]ike prices, privacy relies on competition.").

325. Giovanni Buttarelli, Eur. Data Prot. Supervisor, European Parliament: Address to Socialists and Democrats Group Workshop on the Proposed Digital Content Directive (Jan. 12, 2017), https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf [https://perma.cc/Q4BY-V44V] (criticizing a proposed digital content directive that treated personal data "as a sort of digital currency").

potential federal rights to data privacy. As data privacy develops this more robust societal and legal rights identity in the United States, it has the potential to transform how other areas of law, like antitrust, are able to conceive of and treat data privacy. A new variability will arise as EU-inspired paradigms emerge in certain areas of U.S. privacy law, while older notice and consent laws persist in treating personal data as a commodity. Antitrust law and competition policy will be pressed to reflect a new variety of rights and changes in assumptions in their theories of reconciliation with data privacy.

IV. THE FUTURE OF ANTITRUST LAW AND DATA PRIVACY: DEEPER ANALYSIS, MORE CONFLICTS, AND EXCEPTIONS

So far, this Article contends that antitrust has been too unitary in its treatment of data privacy. It traces a dramatic new variability appearing in the legal identity of U.S. privacy law as it develops a growing number of rights and adopts new prohibitions and duties. It argues that these changes, even if not wholesale across all of U.S. privacy law, are too significant to be ignored by antitrust because they i) erode previously shared assumptions that data-driven competition is positive for consumers, and in doing so, ii) create new variability in how antitrust and data privacy law interact.

This Part outlines important next steps for antitrust law to develop conceptions of data privacy that are more reflective of privacy law itself. First, it calls for antitrust institutions to build their "privacy competency," meaning their willingness to inquire into, and ability to understand, privacy interests and rights. It argues such competency has benefits for both areas of law, and considers practical means to develop it.

Second, and relatedly, it predicts the need for new theories of exception, immunity, and conflict to reconcile antitrust and privacy. It considers, from the antitrust law perspective, how legislatures and courts can begin to conceptualize the scope of such exceptions or immunities for privacy. For courts in particular, it encourages thinking that (i) considers both areas of law relevant in defining the scope of permitted conduct, (ii) seeks to understand the core and edges of the interests of each area of law, and (iii) begins to define what constitutes a conflict between antitrust and data privacy. These ideas are developed by drawing on more established antitrust thinking where it collides with patent rights, free speech rights, and industry regulation. Like privacy law, each of these other areas of doctrine can, at times, protect interests that are incommensurate with competition.

Each of these next steps shares an important paradigm shift: instead of treating privacy as relevant only if subsumed into quality analysis, each addresses privacy as an independent area of legal doctrine in distinct ways. The first emphasizes better recognition of the nature and bounds of privacy doctrine in antitrust contexts. The second emphasizes the development of theories to address tensions, or even conflicts, between the interests protected by data privacy law, and those protected by antitrust law or competition policy.

This is not an argument for a single, new approach to understanding privacy

in antitrust law. That would, ironically, repeat the error of privacy-as-quality theory with overly unitary thinking on how privacy and antitrust interact. There is no single theory that embodies all interactions of antitrust law and privacy, nor should one necessarily be sought. As this discussion has shown, the identity of privacy in the law is multistranded and quickly evolving.[326] The complexity of privacy's legal identity makes it a challenge to trace definitive, normative justification for treatment of privacy one particular way in antitrust law by analogy to its nature in another area of law, right, or regulation. This complexity in privacy's legal identity pushes its treatment toward plurality, in which no analogy to other antitrust thinking fits perfectly, but at the same time, many apply to some extent.

And so, instead of trying to define what privacy is—a definition that privacy law itself has long found elusive—and then attempting to translate that definition into a singular appropriate treatment in antitrust law, this Part instead offers routes to develop deeper and more pluralistic ways of thinking about data privacy in its newest forms. It adds to, rather than replaces, the conception of privacy as quality, which remains useful but, as this Article argues, not sufficient standing alone to account for the changing identities of U.S. data privacy law.

A. Building Data Privacy Competency within Antitrust Institutions

First and foremost, antitrust institutions of all types must develop greater "privacy competency"—a willingness and ability to delve into and understand privacy interests and rights. This includes policymakers, agencies, and courts. Where the two areas of law collide, the antitrust analysis can no longer presume that privacy is relevant only to the extent it can be subsumed into analysis of competitive effects. Instead, antitrust must understand privacy as an independent area of legal doctrine that protects a collection of interests and rights and consider the nature and scope of those protections.

As this Article demonstrates, privacy interests may be dismissed as "not an antitrust issue" or minimized to an extent that becomes inconsistent with privacy law itself. Cases like *hiQ Labs, Inc. v. LinkedIn Corp.* already suggest a tendency to disregard or reduce privacy interests to the point of nonexistence when competition is at stake.[327] The reconciliation of privacy and antitrust where each protects incommensurate values presents a novel conundrum, but narrowing or simplifying privacy as a matter of analytical convenience is not the right solution, particularly where doing so is at odds with privacy law. Instead, antitrust institutions will need a greater willingness to understand the relevance of privacy law to their own mandates and analysis.

---

326. While the law by its nature evolves, the pace of evolution has been dramatic of late for data privacy law. When the drafting of this Article began there were five broad, new state privacy laws. By the end of drafting there were twelve such laws. *See supra* note 272.

327. *See* discussion *supra* Part II. The Consequences of Narrow Privacy Paradigms in Antitrust Law: Unexamined Prioritization of Competition over Data Privacy.

What does it mean for antitrust institutions to develop a greater willingness to delve into privacy? First, it means that, in antitrust contexts, they will have to untangle the specific privacy interests at stake. While privacy law advances no single, unitary interest, that does not mean that the component strands of its identity are unknown. Privacy is many things, but each of those things is known, and so the various threads of "what privacy is" are capable of comprehension in antitrust cases as well.

For example, at times, privacy law protects against intrusion into the private realms of individuals. This can translate to rules that limit the collection of, or access to, personal data. At other times, privacy seeks to protect individuals' interests in how information is used after lawful access to that information is obtained. This can result in rules that, for instance, limit the use of biometric data for commercial purposes, or prohibit data collection in the areas around healthcare facilities.[328]

These different underlying interests, and the rules that protect them, may have differential impacts on competition. If companies are not permitted to collect certain types of data at all, for example, sensitive data about genetic information, then there can be no competition of any type for services related to that data. But if, instead, the privacy rules allow for the collection of that data but prohibit its use for advertising only, then there remains room for competition among services driven by genetic data on the conditions that such services are not ad-supported and data is not resold for advertising purposes. By understanding the nature of what the protected privacy interest is, antitrust law and competition policy can better assess the relevant interaction between privacy law and competition.

As these examples suggest, this new willingness of antitrust to delve into what privacy is requires an understanding of the scope of the privacy interest at stake. Where are the bounds of the privacy right or interest at issue in the antitrust matter? For example, antitrust institutions should understand that the bounds of privacy protection often depend on what type of data is at stake. U.S privacy law has long had stronger protections for children's data, biometric data, health data, and other types of sensitive personal information.[329] On the other hand, where data has been aggregated, anonymized, or made publicly available elsewhere, this can narrow the protected privacy interests, although this will not necessarily mean that no privacy interests exist.

Antitrust will also need to understand that the bounds of protected privacy interests depend on changing conceptions of consent. The lawfulness of data processing has long depended on whether the data subject provided consent, but what constitutes adequate consent is evolving.[330] The new era of privacy law demands recognition that confusing or deceptive consent interfaces are no longer

---

328. See *supra* text accompanying notes 201–208 and accompanying text (discussing biometric and health data geofencing laws, respectively).

329. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 134-35 (2015) (observing there are "special" rules for sensitive information in U.S. privacy law, and discussing examples under COPPA and HIPAA).

330. *See* Part III. A.1. Responding to the Failures of Notice and Consent: Prohibitions and Duties Emerging in U.S. Data Privacy Law.

adequate—what used to be "consent" only in form may no longer suffice to render the processing of personal data lawful.

These examples are general because the analysis of the privacy interests or rights will be highly contextual, depending on the privacy statute, type of data, and nature of data processing at issue on the facts of a particular antitrust matter. The idea is that when privacy is at stake, or may be, antitrust institutions will need to be more willing to wade into the dynamic and evolving existence of privacy law to understand its edges.

Finally, the development of privacy law itself will also play an essential role in clarifying its bounds within antitrust law. Privacy law is in a state of rapid evolution, and antitrust cannot develop a clearer conception of privacy than privacy law itself provides.

As privacy interests become more intertwined with competition, it would be beneficial not just for privacy law itself but also for antitrust courts, legislatures, and the competition side of the FTC to have clearer agency guidance or rules on the scope of Section 5 privacy protections. The FTC is in the midst of its first-ever privacy rulemaking on Section 5 of the FTC Act.[331] While the breadth of this particular rulemaking is controversial,[332] the trajectory toward clear guidance on Section 5 privacy law is positive. The FTC's Section 5 jurisprudence provides the core of privacy protection where sectoral federal statutes do not apply. Yet there is little guidance on the application of this Section for the purposes of privacy protection.[333] The views of the FTC on the scope of Section 5 are also evolving—while the agency once emphasized only the enforcement of company privacy policies, now FTC enforcement goes beyond that to protect consumers reasonable expectations of privacy, even where no express privacy promises were made.[334]

As this Article explains, the United States also has a number of new privacy laws emerging at the state level.[335] The enforcement of these new laws and the passage of the related, first-ever regulations are only just beginning but have great potential to add clarity to the bounds of protected interests in state data privacy law.

---

331. Fed. Trade Comm'n ANPR on Com. Surveillance, *supra* note 197.

332. The rulemaking is pursuant to Section 18 of the FTC Act, 15 U.S.C. § 57a, which authorizes the FTC to promulgate, modify, and repeal trade regulation rules that define acts or practices that are unfair or deceptive in or affecting commerce within the meaning of Section 5(a)(1) of the FTC Act, 15 U.S.C. § 45(a)(1). The broad scope of this rulemaking notice provoked some controversy on the bounds of the agency's authority, see DISSENTING STATEMENT OF COMMISSIONER NOAH JOSHUA PHILLIPS REGARDING THE COMMERCIAL SURVEILLANCE AND DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING 1 (2022).

333. While there is no general guidance on the application of Section 5 of the FTC Act to protect data privacy, the agency recently issued guidance on the specific subissue of Section 5's application to biometric data. *See* FED. TRADE COMM'N., POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf [https://perma.cc/5QVJ-DMJV].

334. Solove & Hartzog, *supra* note 16, at 667 (describing the shift beyond the "broken promises" model of Section 5 FTC Act privacy protection).

335. *See supra* notes 272-282 and accompanying text.

This, in turn, will help to inform the bounds and relevance of those interests to antitrust and other areas of law.

For example, California's Attorney General reached the first-ever settlement under California's Consumer Privacy Act in a 2022 case against makeup company Sephora, Inc.[336] The case alleged that Sephora failed to honor global privacy controls, which are open standards that allow end users to signal their opt-out privacy preferences across various contexts through a browser extension or setting. These technology-driven decisions to opt out of data processing have the potential to replace the friction of individualized consents that are proliferating online. Before this enforcement, there was some question as to whether California law required companies to treat global privacy controls as valid and binding opt outs.[337] The settlement, while not binding on other parties, provides useful clarification. The State Attorney General views these privacy preferences as binding and will require companies to honor global privacy controls used by individuals to convey preferences around the sale and sharing of personal information.[338] New rulemaking under California state law further confirms this position, requiring such controls to be honored.[339]

This clarification of the law is relevant to understanding privacy within antitrust analysis. Imagine a dominant firm that terminates the access of a third-party rival to its social media platform, ending that rival's ability to process competitively valuable personal information about end users obtained via that platform. Evidence shows that the reason for the termination was the third party's repeated failure to honor end users' global privacy controls. This dominant firm competes in the marketplace for social media services based on its reputation for strong privacy protections. The excluded rival may still bring an antitrust case in an attempt to restore data access, but it's clear violation of data privacy law gives the dominant firm a strong justification for its conduct: the termination was important to both the firm's privacy law compliance, and its related competitive value proposition in the market.[340]

Finally, antitrust institutions must not just be willing to inquire into privacy interests but also able to do so. Here, privacy experts will play an important role. Privacy scholars, civil society, practitioners, and agencies themselves (or Bureaus, as at the FTC) are in the best position to help antitrust courts and lawmakers analyze data privacy correctly. It is well worth their time to contribute privacy expertise as

---

336. *See* Press Release, Cal. Dep't of Just., Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement [https://perma.cc/EKS9-U6J5] [hereinafter "California CCPA Settlement with Sephora"].

337. *See, e.g.*, Omar Tene, *The Sephora case: Do not sell–But are you selling?*, IAPP (Aug. 29, 2022), https://iapp.org/news/a/the-sephora-case-do-not-sell-but-are-you-selling/ [https://perma.cc/35B3-DHWW] (calling the California legislation "vague" on the respect to recognition of such signals).

338. California CCPA Settlement with Sephora, *supra* note 336.

339. California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–1798.199.

340. *See* Erika M. Douglas, *Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis*, 97 NOTRE DAME L. REV. REFLECTION 430 (2022) (analyzing when privacy protection is cognizable as a justification in antitrust).

amici, experts, and policy commentators in the antitrust context because, as this Article argues, conceptions of data privacy are not neatly cabined within antitrust decisions.[341] Misapprehensions of data privacy can spread through the common law from antitrust cases outward to data privacy jurisprudence, weakening privacy interests and rights as interpreted by courts in standalone privacy cases as well.

In particular, it will be essential for privacy enforcers and antitrust enforcers to collaborate on matters that implicate both areas of law.[342] Whether cross-Bureau, as at the FTC, or cross-agency, as is more common internationally,[343] there is a new imperative for the entities tasked with antitrust enforcement to collaborate closely with the entities tasked with privacy enforcement. In digital spaces where personal data drives competition, privacy and competition will be inextricably linked such that neither agency can effectively intervene without the insights of the other. The importance of such privacy and antitrust collaboration is already being emphasized in global conversations and action,[344] and, outside the United States, is manifesting in the establishment of several new national fora created to facilitate collaboration across the doctrinal bounds of privacy and competition law.[345] Antitrust enforcers will never understand privacy to the same extent as privacy enforcers, nor is there a need for them to do so. What is needed is the ability to assess and recognize when the input of privacy experts is required to answer the sorts of questions outlined above. Then, it will be for antitrust authorities to decide the relevance of that clear and accurate privacy analysis to their own assessments.

Getting privacy correct matters to antitrust law because it helps to ensure an appropriately broad application of antitrust where it meets countervailing privacy

---

341. *See* discussion *supra* Part II. The Consequences of Narrow Privacy Paradigms in Antitrust Law: Unexamined Prioritization of Competition over Data Privacy.

342. See generally further discussion of this collaboration imperative in Erika M. Douglas, *Constructing the Digital Regulatory Ecosystem: Agency Collaboration*, 26 VA. J.L. & TECH. 1 (2023).

343. The more common model globally is to have separate agencies for the enforcement of antitrust law and privacy law, unlike the United States, which houses both functions within the FTC, albeit in separate Bureaus.

344. *See*, *e.g.*, Melanie Drayton & Brent Homan, *Regulating The Digital Economy – Why Privacy And Competition Authorities Should Talk To Each Other*, TECHREG CHRONICLE 4 (2022), https://globalprivacyassembly.org/wp-content/uploads/2023/03/Annexe-2-DCCWG-2022-AR-Regulating-the-Digital-Economy-Competition-authorities-should-talk-to-each-other-Melanie-Drayton-Brent-Homan-3.pdf [https://perma.cc/H7ZX-GPN2] ("[C]ollaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.").

345. GLOBAL PRIVACY ASSEMBLY, DIGITAL CITIZEN AND CONSUMER WORKING GROUP REPORT 48, 51 (2023) https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-DCCWG-Annual-Report-2023-2023.09.281.pdf [https://perma.cc/2UVN-QUB9] (noting the establishment of a new Canadian Digital Regulators Forum and Australian Digital Platform Regulators Forum to enable collaboration among competition, privacy, and consumer protection enforcers). The U.K. privacy and competition authorities established a similar Digital Regulation Cooperation Forum in 2020. *See Digital Regulation Cooperation Forum,* ICO, https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/ [https://perma.cc/AC6W-F5JS] (last visited Apr. 13, 2024). The EU started a similar initiative in 2016-2017 see *Background*, DIGIT. CLEARINGHOUSE, https://www.digitalclearinghouse.org/#:~:text=Background,protection%2C%20consumer%20and%20competition%20law [https://perma.cc/D9CD-Z8GQ] (last visited Apr. 13, 2024).

interests. Consider, as an example, the growing number of arguments by antitrust defendants that the protection of users' privacy justifies otherwise anticompetitive conduct. In cases where an antitrust plaintiff has made a *prima facie* showing that the defendant's conduct is anticompetitive,[346] the defendant is then afforded the opportunity to demonstrate a procompetitive justification—to provide proof that, upon closer examination, the conduct is actually procompetitive.[347] Defendants have now begun to claim that privacy protection constitutes such a justification. Apple successfully made this argument in recent litigation in the Ninth Circuit,[348] and LinkedIn claimed such a privacy justification in *hiQ Labs, Inc. v. LinkedIn Corp.*[349]
In a twist on this issue, a group of state attorneys general have sought to preempt such an argument by technology giant Google by arguing in their complaint that Google's anticipated privacy excuses are "a ruse" and mere "pretext" for the alleged anticompetitive conduct.[350]

The recent Ninth Circuit decision involving Apple was the first to recognize privacy-based procompetitive justifications in antitrust law.[351] Courts and agencies seeking to apply this law to assess privacy justifications will have to determine the veracity or pretext of the privacy interests being invoked.[352] Are the defendant's claims of privacy justifications, in fact, positive for competition? Or is the "justification" merely privacy pretext, used by the defendant as cover for its anticompetitive conduct? It is fundamentally important for antitrust to get this analysis right, because the establishment of a justification will often affect the outcome of the antitrust case.[353] If a justification is shown, the defendant is unlikely to be found

346. United States v. Microsoft Corp., 253 F.3d 34, 59 (D.C. Cir. 2001) (per curiam) (describing the burden-shifting framework for the rule of reason). The rule of reason is the most commonly applied analytical standard in assessing anticompetitive conduct in antitrust law.

347. *Id.* at 59 (describing a procompetitive justification as "a nonpretextual claim that [the monopolist's] conduct is indeed a form of competition on the merits because it involves, for example, greater efficiency or enhanced consumer appeal." (emphasis added)).

348. Epic Games, Inc. v. Apple, Inc., 67 F.4th 946, 985-86 (9th Cir. 2023) (affirming the district court finding that Apple offered nonpretextual, legally cognizable procompetitive justifications for the challenged rules regarding app distribution and payment. One of the accepted justifications was that the rules "improve device security and user privacy—thereby enhancing consumer appeal and differentiating iOS devices and the App Store from those products' respective competitors").

349. *See supra* text accompanying footnotes 107-113.

350. Second Amended Complaint, Texas v. Google LLC, No. 20-CV-957, 2021 WL 2043184, 60, 96–99 (E.D. Tex. Aug. 4, 2021) (alleging that Google's planned termination of third party cookies access to its Chrome browser is anticompetitive because it "raise[s] barriers to entry and exclude[s] competition in the exchange and ad buying tool markets" by blocking cookies tracking by publishers and advertisers, who would otherwise compete with Google to deliver advertising). The content s of the complaint suggests Google is expected to argue that its cookies policy change protects the privacy of users by limiting third-party access to users' online tracking data. *Id.*

351. *Epic Games, Inc.*, 67 F.4th at 985-86.

352. While the pretextuality inquiry is used here as a rough analogy for the inquiry that will be conducted into the veracity of privacy interests, this is not to imply that standing alone, privacy protection is a justification for antitrust misconduct. *See* Douglas, *supra* note 340, at 466–70 (explaining that to constitute a justification in antitrust law, privacy protection must also enhance competition).

353. *See id.* at 431 (explaining how the establishment of a justification can determine the outcome of a rule of reason antitrust case).

liable for a violation of antitrust law.[354] If instead, the privacy justification is found to be pretextual, the defendant is likely to face antitrust liability.[355]

As scholar Rory Van Loo observes in other legal contexts, the expansive definitions and multifaceted identity of privacy have left it "vulnerable to obfuscation" and thus capable of being used as a pretextual excuse or shield for misconduct.[356] In employment litigation and securities fraud cases, he observes defendants invoking the privacy interests of others—employees in one instance and bank customers in another—as pretext to resist disclosure in discovery.[357] A similar risk of obfuscation may arise in antitrust law when data privacy enters into the analysis—the less clear the parameters of privacy law are, the more likely a defendant can use privacy as a façade to shield anticompetitive conduct from proper antitrust scrutiny.

The more competent antitrust law and its institutions are at understanding privacy—and its bounds—the less risk there is of such obfuscation. Continuing the example above, the correct antitrust analysis of privacy justifications depends on precisely the sort of privacy competency argued for in this Article. Antitrust institutions that understand data privacy are less likely to be misled by defendants' exaggerated claims of privacy interests being used as a ruse to block competition. Only by delving into the nature and scope of privacy interests, with the help of privacy experts, can antitrust institutions guard against the unnecessary sacrifice of competition for privacy pretext.

Courts and agencies will have to assess whether the impugned conduct implicates a privacy interest or right. This may often involve considering whether privacy law protects the claimed interest or right by looking to the relevant privacy legislation, common law, and its enforcement to understand whether the conduct involves protected interests. Decisions like *hiQ Labs, Inc. v. LinkedIn Corp.*[358] have been skeptical of such privacy interests when invoked by a defendant even though, upon a closer look, those interests are protected to at least some extent by privacy law.[359]

The defendant's own conduct and documents will also be useful to courts seeking to assess whether the claimed privacy interests are pretextual. While the evidence will vary by case, relevant considerations may include contemporaneous documents of the defendant that discuss privacy interests, and the defendant's terms and practices in enforcing its privacy policy. In a leading Canadian case on privacy as a procompetitive justification, *Commissioner of Competition v. Toronto Real Estate Board*, the competition tribunal found the defendant's consent practices around

354. *Id.*

355. *Id.*

356. Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 168 (2022).

357. *Id.* at 134.

358. hiQ Labs. v. LinkedIn Corp., Inc., 31 F. 4th 1180, 1189–90 (9th Cir. 2022), *order dissolved on other grounds* No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022).

359. *Id.* at 1194 (conceding that posting publicly on social media may not imply consent to the use of data for "all purposes," but ultimately agreeing with the district court that user privacy expectations in all public LinkedIn profile information were "uncertain at best").

personal data use prior to the litigation were revealing.[360] The defendant claimed its anticompetitive conduct was justified by the need to protect individuals' privacy interests. But the defendant had interpreted its privacy policy more broadly to its own advantage in similar matters prior to the litigation.[361] The more stringent interpretation of the policy in the instant case suggested that the consumer privacy interests being invoked were pretextual, a late-stage effort to defend against the antitrust claims.[362] As this reflects, documents and practices around privacy can be useful for assessing whether a privacy interest is implicated not just in law but on the specific facts of the case. Simply because privacy rights or interests *exist* in law does not mean they are necessarily impacted by alleged anticompetitive conduct. The tribunal in *Toronto Real Estate Board* ultimately concluded that the defendant's claims of privacy protection were an "afterthought and continue to be a pretext" in the face of litigation.[363]

When conducting these sorts of inquiries, courts could benefit greatly from the expert opinions of privacy enforcers, scholars, and civil society organizations on whether a privacy interest is at stake. This requires the sort of collaboration called for above. Once the reality or pretext of privacy interest is understood, the antitrust analysis will need to continue, to assess the relevance to competition. This is a judgment in antitrust rather than privacy, and is necessary to conclude whether a justification is established.[364]

This example of justifications analysis shows that, as privacy law proliferates and gains in legal stature, it will press antitrust, courts, legislators, and agencies into assessing whether privacy interests or rights are truly at stake or merely pretext to avoid competition. This issue is new and important to the intersection of antitrust law and data privacy. Such assessments have the power to determine the outcome

360. Comm'r of Competition v. Toronto Real Est. Bd., [2016] Comp. Trib. 7, 7 (Can.). The association had passed rules of conduct that excluded new, online brokers, who competed at lower prices than traditional brokers, from accessing listings with photos of homes for sale. In the face of a complaint by the Canadian competition enforcers that the rules violated competition law, the defendant association argued the rules were necessary to protect home seller's privacy. *Id.* ¶¶ 10–14.

361. *Id.* ¶¶ 405–06. In other business contexts, the defendant had interpreted preexisting consumer consents as sufficiently broad to enable its own disclosure of personal data. When it came to the anticompetitive restraints challenged in the case, though, the defendant interpreted its consent obligations more strictly, invoking those obligations as a reason to limit data access for online brokers. *See id.* ¶ 406. Further, the documentary evidence showed that when the defendant realtor's association faced earlier (unrelated) privacy concerns over the online posting of interior home photos, it sought legal advice, then modified its standardized listing agreements to include consent to such postings. *Id.* Yet the defendant took no equivalent action to address the privacy concerns that were asserted as a justification in the instant case for its anticompetitive acts. This discrepancy suggested that privacy was not, in fact, at stake in the defendant's disputed decision to block certain online brokers' access to home listing data. *Id.*

362. *Id.*

363. *Id.* ¶ 390.

364. Douglas, *supra* note 340, at 466–70 (explaining antitrust analysis of pretextual justifications, including those related to privacy).

of the antitrust case and so go to the core of reconciling the two areas of law effectively. If a pretextual privacy justification is accepted for anticompetitive conduct, then antitrust law has sacrificed competition where it should not have. To correctly assess whether a privacy right or interest is at stake, it will be important for antitrust enforcers, courts, and even legislatures to develop their willingness to understand and collaborate at intersections with privacy law.

B. Defining Conflicts and Exceptions in Antitrust Law for Data Privacy—Legislative and Judicial Roles

Once the nature and scope of the privacy interests are understood with clarity, the next step in the analysis will depend on whether those interests are complementary or instead truly at odds with competition. In the easy cases, the interests protected both by antitrust law and data privacy law will be jointly served. Such complementarity might be achieved by making adjustments that come at little to no cost to the other area of law. For example, in some markets, robust data-driven competition may be possible based on access to reliably anonymized personal data. Instead of ordering access to identifiable personal data, antitrust law could mandate access to anonymized data instead. This could achieve or maintain competition while still protecting data privacy. As another example, imagine a merger that might otherwise harm advertising competition because it enables the combination of large and unique troves of personal health data that rivals cannot match. The transaction could be allowed to proceed in antitrust law under the condition that certain data be siloed off to prohibit its use in advertising.[365] This antitrust solution is likely to have incidental privacy benefits because it prevents that health data from being used in targeted advertising by the merged company. Both competition and privacy are protected.

The more difficult scenarios, and the focus of this Section, are those that give rise instead to true tension or conflict between antitrust and privacy interests or rights. These scenarios present a much more challenging dilemma for legal institutions than situations of complementarity. Where privacy law is truly at odds with antitrust law, one area or the other will ultimately have to cede.

This Section explores how such tensions or conflicts are likely to press courts and legislatures to develop new theories of exceptions or immunity at intersection of antitrust and privacy. It addresses the ways in which antitrust law can begin to address this challenge, first legislatively and then judicially. As with the proposal above to build privacy competency, this development of exceptions is an important

365. An example of such a data silo appeared in the European Commission's approval of the Google/Fitbit acquisition. As a condition of Google's acquisition of this fitness tracking company, the European Commission ordered that post-merger the personal data of end users collected by Fitbit be held separately from Google's data and not combined for the purpose of advertising. Press Release, European Commission, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Condition (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 [https://perma.cc/LF8P-HH28].

paradigm shift at the interface of antitrust law and privacy. It reflects a recognition in antitrust law that, as a distinct and separate area of doctrine, data privacy law can, at times, protect rights or interests that are incommensurate with competition.

While this Section considers the antitrust perspective on exceptions and immunities for privacy, at times the inverse may be needed—privacy law exceptions to enable competition. This raises policy questions beyond those addressed in this Article: when it would be socially beneficial or desirable to prefer competition over data privacy, or vice versa, and what criteria might be applied to make that determination? This Article has so far contended that the de-prioritization of privacy in favor of competition should be analyzed and justified expressly, rather than assumed. Its primary focus is not on deciding when each interest should prevail but rather on reaching the point of such decision-making through analytical approaches that reveal such questions. The goal is to set out analytical precepts for how courts and legislatures might begin to identify and analyze the potential for conflicts and the possible need for privacy exceptions in antitrust law. This Article leaves views on the appropriate balance between competition and privacy for later analysis, and leading privacy scholars have begun to address such policy questions.[366] Perceptions of the 'right' balance between these interests are likely to vary with political views and with specific context.

1. Legislative Exceptions in Antitrust for Privacy

When federal antitrust law, as it exists or as it develops at this interface, is in conflict with privacy law or policy, Congress will have a decision to make. Which interest should be elevated over the other—competition or privacy? Congress can choose to authorize behavior that improves privacy but would otherwise violate antitrust law, or vice versa. At times, there will be a preference for competition over privacy, and privacy legislation will need to include exceptions to enable competition. At other times, there will be a preference for privacy over competition, such that antitrust legislation will have to incorporate exceptions for privacy. The latter is considered here.

Congress has created other exceptions to antitrust law to advance various socioeconomic interests, and it has the power to do the same for privacy. For example, agricultural producers are exempted from antitrust law to permit joint selling,[367] which would otherwise constitute an unlawful cartel. This is permitted as a matter of policy to help agricultural producers counteract the market power of their buyers. Legislative antitrust exceptions have been created to permit market division in the production of military materials during times of national

366. *See generally* Peter Swire, *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations*, 6 GEO. L. TECH. REV. 57 (2022) (providing a framework to assess issues of data portability and other required transfers of data that includes impacts on competition, privacy, and cybersecurity).

367. Capper-Volstead Act, 42 Stat. 388 (1922) (codified at 7 U.S.C. § 291).

emergency.[368] Collective resident matching programs are permitted for medical graduates,[369] among a handful of other exceptions that seek to achieve socially desirable outcomes not thought possible in competitive markets.[370]

Perhaps most analogous to the antitrust/privacy interface, Congress has made the choice to prioritize certain privacy protections in bankruptcy law divestitures. When a bankrupt entity's assets include valuable personal information about individuals, a tension can arise with data privacy. The debtor and its creditors are interested in maximizing the value recovered from selling that personal data as an asset in bankruptcy. This meant bankruptcy trustees were allowing the sale of personal data to the highest bidder, regardless of the bidder's privacy *bona fides*, and despite such sales being in violation of the original company's privacy policy.[371] Individuals' interests in controlling who purchased and gained access to their personal information were being disregarded in order to obtain a high price for that personal data in bankruptcy proceedings. Congress intervened in 2005, amending the Bankruptcy Code to require that such sales of data comply with the debtor's privacy policy or with privacy law.[372] This provided at least some privacy protection for individuals whose personal information was auctioned off in bankruptcy proceedings, in exchange for a potential decrease in the value that debtors could recover from such data sales.[373]

At times, Congress may similarly choose to prioritize privacy over competition in antitrust legislation. For example, it could be beneficial to permit companies in the same industry to collectively set technical standards for data portability to ensure that data can be moved between services. Without a clear antitrust exception, this collaborative conduct could bring antitrust law scrutiny. Congress could choose to exempt such cooperation among competitors to achieve data portability standards that promote individual control over data and data privacy protection.

Today, novel exceptions for data privacy are just beginning to emerge in proposed federal antitrust bills. The American Innovation and Choice Online Act and similar bills seek to impose interoperability obligations on large digital

368. 50 U.S.C. § 4558(j).

369. 15 U.S.C. § 37b (confirming the antitrust immunity of matching programs).

370. *See* AMERICAN BAR ASS'N, FEDERAL STATUTORY EXEMPTIONS IN ANTITRUST LAW 31–52 (2007) (describing an array of legislative exceptions from antitrust law).

371. Complaint ¶ 10, Fed. Trade Comm'n v. Toysmart.com, No. 00-11341 (D. Mass. July 10, 2000).

372. Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109-8, § 231, 119 Stat. 23, 72−73 (2005) (codified as amended at 11 U.S.C. § 363(b)(1)) (amending section 363(b)(1) of title 11 of the United States Code to include restrictions on a debtor's ability to transfer personally identifiable information when a privacy policy restricts its transfer). When the debtor has a privacy policy that prohibits the transfer of personally identifiable information that is being sold or leased as an asset, such a transfer is allowed in bankruptcy only if the transfer is (i) consistent with that debtor's privacy policy or, (ii) after appointment of a privacy ombudsperson, the transfer is approved by a court that finds it would not violate privacy law (or other "non-bankruptcy" law). 11 U.S.C. § 363(b)(1).

373. *But see* Christopher G. Bradley, *Privacy for Sale: The Law of Transaction in Consumer's Privacy Data*, 40 YALE J. ON REG. 127, 194–95 (2023) (observing that these protections afforded in bankruptcy are limited by the frailties of data privacy law itself).

platforms.[374] Under several of these proposed laws, large digital platforms would be required to allow certain rivals to interconnect with their services on terms equivalent to the platform's own vertically integrated businesses.[375] The goal of these proposed laws is to promote and restore competition in online services such as shopping, search, and social media.[376]

The effect, however, may also be to allow much greater access to the massive amounts of personal data held by these large digital platforms.[377] The mandated interoperability contemplated by these laws is intended to do exactly this—give online rivals access to data so they can use that data to compete. This and other similar bills therefore include exceptions and defenses to relieve the platforms of interoperability obligations when doing so is required to protect end users' data privacy and security.[378]

In some sense, the appearance of these privacy exceptions reflects progress. Just a few years ago, it was unlikely these antitrust-inspired bills would have referenced data privacy at all. The inclusion of such exceptions demonstrates that data privacy is rising in its legal strength and stature, leaving antitrust little choice but to contemplate privacy defenses at the legislative level.

In another sense, these bills reflect the undeveloped state of antitrust treatment of privacy that is lamented throughout this Article. The exceptions tend to lack depth or nuance in their treatment of privacy. The American Innovation and Choice Online Act, for example, refers to the term "privacy" without defining or explaining it—despite the notorious ambiguity of privacy as a concept.[379] There is also little articulation of the anticipated scope of privacy exceptions.[380] If these or similar laws pass, it will leave important, unanswered questions about when the exception may apply: Is there a privacy defense for denying interoperability when a competitor violates the platform's privacy policy? Or must there be a violation of blackletter privacy law before the defense applies?[381] In broader terms, what constitutes a privacy interest adequate to relieve platforms of their otherwise

374. *See supra* text accompanying footnotes 149-154 (discussing the American Choice and Innovation Online Act and similar legislation).

375. *Id.*

376. *Id.*

377. *See generally,* Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J. L. & TECH. 2, 60 (2020) (discussing the important role of consumer data, including personally identifiable information, in digital platform businesses and competition).

378. *See supra* text accompanying footnotes 154-158 (discussing the American Choice and Innovation Online Act and similar legislation).

379. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021–2022).

380. *Id.*

381. For example, in the context of bankruptcy law either compliance with the relevant privacy policy or a determination of law is adequate to permit the transfer of personal information. When the debtor has a privacy policy that prohibits the transfer of personally identifiable information that is being sold or leased as an asset, such a transfer is allowed in bankruptcy only if the transfer is (i) consistent with that debtor's privacy policy or, (ii) after appointment of a privacy ombudsperson, the transfer is approved by a court that finds it would not violate privacy law (or other "non-bankruptcy" law). 11 U.S.C. § 363(b)(1).

legislated obligations to allow access to user data? While courts can be expected to develop some metes and bounds of legislative exceptions, these are significant holes to fill. It reflects the need for legislators to develop a greater willingness and ability to inquire into and understand the scope of "privacy" as it relates to antitrust and competition laws.

2. Judicial Thinking on Conflicts, Exceptions, and Immunities for Data Privacy in Antitrust Law

As data privacy increases in strength and stature within U.S. law, it will press antitrust to consider exceptions to accommodate the rights and interests that law protects. Antitrust has long been developed through the common law more so than by legislative change,[382] and that is likely to be true where it meets privacy as well. Where antitrust legislation is silent as to whether competition or privacy law should prevail—as all antitrust law is right now—the courts will play an important role in defining conflicts, exceptions, and immunities between these areas of law.

This Section first considers the bounds of this judicial role. Then, within those bounds, it proposes three analytical approaches to help courts to begin conceptualizing new tensions, exceptions, and conflicts between antitrust law and privacy. It calls for courts to (i) consider both areas of law relevant in defining the scope of permitted conduct, (ii) seek to understand the core and edges of the interests protected by each area of law, and (iii) begin to define what constitutes a conflict between the two areas of law. Judicial doctrine on antitrust and data privacy is nascent, and so the argument here draws analogies to other areas where antitrust doctrine collides with incommensurate interests, in the law of patent, free speech, and industry regulation. While none are a perfect analogy to privacy rights and interests, each offers insight into how antitrust courts navigate countervailing legal interests.

a. Understanding the Judicial Role in Creating Antitrust Exceptions for Privacy

There are important limits to the judicial role in determining whether privacy or competition prevails. In antitrust law, the Supreme Court has confirmed that Congress, not the courts, should dictate when competition yields to other public policy priorities, such as safety or health.[383] The assumption in antitrust law is that competition is positive for consumers, even if countervailing social interests, like health or safety, may be harmed by increased competition.[384] Antitrust can be limited by other areas of legal doctrine, but the courts cannot decide on their own accord that competition is problematic and should be limited to achieve other socially beneficial interests. While this limit on the judicial role can be frustrating for

382. Northwest Airlines, Inc. v. Transport Workers, 451 U.S. 77, 98 n. 42 (1981) ("In antitrust, the federal courts . . . act more as common-law courts than in other areas governed by federal statute.").

383. Nat'l Soc'y of Pro. Eng'rs v. United States, 435 U.S. 679, 695 (1978).

384. *See* discussion *supra* Part I.C. (explaining that the legislative scheme of the Sherman Act precludes inquiry into whether competition is "good" or "bad"; instead, it assumes that competition improves consumer welfare).

those who seek to use antitrust law to advance privacy or other social interests in contexts unrelated to competition, it is well established.

This limit on the judicial role in antitrust, however, does not preclude courts from reconciling different areas of legal doctrine. They have often done so where antitrust efforts to promote competition collide with other areas of law that can have the effect of limiting competition, such as patent law, free speech rights, and industry-specific regulation, each of which is analogized in the discussion here. Courts address these areas of law not in the capacity of deciding policy trade-offs but in developing theories to reconcile interacting areas of law. In sum, courts have the power to examine privacy law where it interacts with antitrust law, provided their decisions are not an expression of mere policy preference.

This thinking is, in itself, a shift from privacy-as-quality treatment. Instead of subsuming privacy into antitrust law only when it relates to competitive effects, it places privacy on more equal footing to consider how, as an area of law that protects incommensurate interests, it may at times be in tension or conflict with antitrust law.

b. Both Antitrust and Privacy Law Define Permitted Conduct: Analogies to the Patent Interface

As I have argued elsewhere, when antitrust and privacy law collide, courts should consider both areas of law relevant to understanding the scope of permitted conduct.[385] This thinking draws on analogies from the reconciliation of antitrust with patent law.[386] Patents confer a lawful right to exclude competition, and that lawful exclusion is beyond the purview of antitrust law. However, more nuanced approaches to reconciling antitrust with patent law are needed because patent holders, at times, abuse their patents in ways that stray beyond the bounds of this lawful right to exclude and unduly disrupt competition. A rightsholder might interpret their patents as overly broad to block rivals, to force buyers to purchase a tied but unpatented product,[387] or they may pay competitors to stay out of the market after their patent expires. [388] In each case, antitrust has intervened to rein in the abuse of patent rights and protect competition.

This is a careful balance—if antitrust law oversteps and impedes efficient, legitimate uses of patent rights, it can undermine the incentives that patent rights offer to drive innovation. Conversely, if patent rights are misunderstood as overly broad, they can block competition unnecessarily by giving the patent holder rights

385. Douglas, *supra* note 43, at 680–83.

386. FTC v. Actavis, Inc., 570 U.S. 136, 136 (2013).

387. *See e.g.* Int'l Salt Co. v. United States, 332 U.S. 392 (1947) (tying of patented canning machinery to unpatented salt as a condition of purchase poses an unacceptable risk of stifling competition and is unreasonable per se).

388. FED. TRADE COMM'N, THE EVOLVING IP MARKETPLACE: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION 1 (2011), https://www.ftc.gov/sites/default/files/documents/reports/evolving-ip-marketplace-aligning-patent-notice-and-remedies-competition-report-federal-trade/110307patentreport.pdf [https://perma.cc/XBU8-TFT3]; *See, e.g.*, *Actavis*, 570 U.S. at 149 (rejecting the "scope of patent" approach that had immunized many reverse payment settlements from antitrust scrutiny).

not actually afforded by patent law. In navigating this intersection, recent Supreme Court jurisprudence has thus emphasized an "accommodation" between the two areas of law, in which both patent and antitrust policies are relevant to determining the scope of permitted conduct by a patent rights holder.[389] Where the two collide, neither one nor the other solely establishes the lawful conduct.

Where antitrust meets privacy rights, courts should similarly treat both areas of law as relevant to determining the scope of permitted conduct. For example, if defendants are able to use pretextual privacy interests to justify their anticompetitive conduct, that limits competition unnecessarily because it is beyond what privacy law actually requires. It overinterprets the breadth of privacy rights or interests at the cost of competition. When courts understand the true scope of privacy law protection, it can help to avoid such a result in antitrust law.[390] And conversely, if antitrust misunderstands privacy protection as too narrow, it could order conduct that privacy law prohibits. For example, an antitrust court might require the divestiture of competitively important data that is also personal and sensitive, as part of a merger remedy. Data privacy law may prohibit such a sale of the information without consent. Both areas of law affect their reconciliation. This is a shift from existing antitrust theory, which conceives of privacy as an element of quality subsumable into the antitrust analysis. It instead elevates the countervailing interests protected by privacy law to help determine the permitted conduct where the laws intersect.

c. Assessing the Centrality of Protections in Antitrust Law and Privacy Law: Analogies to the Free Speech Interface

Antitrust law has also developed rich theories to address its collision with incommensurate free speech rights.[391] This thinking offers another useful analogy for reconciling antitrust and privacy where the two collide, one that commends judicial consideration of how central each of the protected interests at stake are, respectively, to antitrust law and to data privacy law.

The freedom of speech guaranteed by the First Amendment of the Constitution interacts with antitrust law when such speech is used to harm competition.[392] Viewed collectively, the antitrust jurisprudence on free speech suggests a legal recognition that each area of doctrine has a core and also edges. This distinction helps to inform which area of law will prevail.

At one extreme, antitrust law has crafted exceptions or read down the scope of the Sherman Act to avoid a conflict with speech rights when the impugned

---

389. *Actavis*, 570 U.S. at 137.

390. *See infra* discussion in text accompanying footnotes 356–364.

391. *See* Hillary Greene, *Muzzling Antitrust: Information Products, Innovation and Free Speech*, 5 B.U. L. REV. 35 (discussing the theories and challenges of antitrust law where it collides with incommensurate interests in free speech and patent law).

392. *See e.g.*, FTC v. Superior Ct. Trial Laws. Ass'n, 493 U.S. 411 (1990); NAACP v. Claiborne Hardware Co. 458 U.S. 886 (1982).

conduct in an antitrust case places the values that animate free speech rights squarely at stake. The *Noerr-Pennington* doctrine holds that the Sherman Act, one of the most important federal antitrust statutes, does not prohibit collective political lobbying by competitors, because such legitimate efforts to secure government action are an essential form of protected speech.[393] Even if the lobbying involves cooperation between competitors that reduces competition—conduct that antitrust law would otherwise prohibit—the central importance of political speech prevails and antitrust law allows the lobbying.[394]

At the other extreme, however, the law is clear that the First Amendment does *not* shield from antitrust scrutiny speech that is tangentially involved in misconduct the Sherman Act squarely prohibits. The Supreme Court has found that there is no protected right of competitors to engage in speech in service of an unlawful antitrust conspiracy.[395] All unlawful conspiracies involve some incidental speech among competitors as they communicate to reach an agreement on the prices to be fixed or engage in other forms of unlawful collusion. In *FTC v. Superior Court Trial Lawyers Association*, the Supreme Court found that this incidental need for speech to reach a conspiracy agreement was not adequate to shield every unlawful conspiracy from Sherman Act scrutiny.[396] Antitrust laws still apply when competitors engage in speech that is used "to increase the price that they would be paid for their services," rather than for protected purposes, such as to urge political action by government.[397] Such agreements among competitors to fix prices are a classic violation of the Sherman Act at the very core of antitrust law,[398] while the speech interests at stake in forming an unlawful commercial conspiracy are marginal to First Amendment protections.

In navigating the interactions between antitrust and data privacy, courts should engage in similar analysis, asking how central the interests at stake are to each area of law.[399] Where antitrust courts face the task of reconciling incommensurate

---

393. The doctrine is named for cases in which it was established, United Mine Workers of Am. v. Pennington, 381 U.S. 657, 670 (1965); E.R.R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127, 135 (1961).

394. *Id.*

395. *See also* Nat'l Soc'y of Pro. Eng'rs v. United States, 435 U.S. 679, 697 (1978) (explaining order enjoining the engineers from publishing ethical opinions opposing competitive bidding does not infringe the First Amendment, even though the "injunction against price fixing abridges the freedom of businessmen to talk . . . about prices").

396. *Superior Ct. Trial Laws. Ass'n*, 493 U.S. 411 (group of state-compensated attorneys engaged in a concerted refusal to accept new legal cases until the state paid them higher compensation; the speech at issue was not protected by the First Amendment).

397. *Id.* at 427.

398. PHILLIP E. AREEDA & HERBERT HOVENKAMP, FUNDAMENTALS OF ANTITRUST LAW § 19.03 (4th ed. 2023) ("Horizontal agreements are antitrust's most 'suspect' classification, and as a class provoke harder looks than any other arrangement.").

399. This analogy is not equating the legal standing of data privacy rights to those of free speech rights in law. Each right has a particular legal identity that informs its treatment. The constitutional protection of free speech rights strengthens the case for their exception from antitrust law when conflicts arise, though at times antitrust law still prevails. The federal data privacy laws discussed here

privacy interests, on one hand it is useful to understand how central the data interest being invoked is to privacy law protection, and, on the other hand, how significant the impact of the alleged misconduct is to competition. When one interest is central to the protections afforded by that area of law and the other is not, that weighs in favor of preferring and protecting the central interest.

As an example of this, consider a cartel in which members agree to exclude upstart competitors from the supply of valuable, personal user data that is required to compete in the relevant antitrust market. Combatting cartels is at the core of antitrust law, which has long barred horizontal agreements on price and other aspects of competition that exclude rivals.[400] The cartel members claim that their exclusionary conduct is justified because limiting those rivals' access to this data improves user privacy, which users value, and this helps the cartel members to compete. If access to the personal information at issue could enable competition even when reliably anonymized or aggregated, then the data privacy interest at stake are likely marginal. The claim of privacy protection is unlikely to be supported in fact or to justify the conduct in antitrust law. But if instead the data at stake is biometric information—which is becoming among the more sensitive types of personal data and is subject to recent state and federal action to protect against certain commercial uses[401]—then the privacy interest claimed by the defendants is much closer to the core of data privacy law and should be more carefully scrutinized by the court. The cartel's justification becomes more plausible, though the causal connection to competition and the exclusionary conduct would still have to be shown. The centrality of the interest at stake to privacy law informs the antitrust analysis.

d. Defining Conflicts in Antitrust with Privacy Law: Analogies to the Regulatory Interface

Finally, in thinking about judicial immunity for privacy in antitrust law, it is useful to consider one area of antitrust treatment of incommensurate interests: where it meets industry regulation. Some regulatory regimes are complementary to antitrust law, with a shared emphasis on competition. Other types of regulation sacrifice competition to achieve other socio-political goals that are not thought achievable in competitive markets, as in the example above of agricultural cooperatives. Sometimes Congress will indicate in the legislation whether antitrust or the regulation takes priority with either an antitrust savings clause or a preemption clause.

---

lack similar constitutional moorings, though adjacent areas of data privacy law are constitutional in nature. *See, e.g.*, The constitutional dimensions of data privacy law on display in cases like Carpenter v. United States, 138 S. Ct. 2206 (2018) (considering Fourth Amendment rights in cell phone location data used by law enforcement), and recent changes in U.S. privacy law have been influenced by European constitutional conceptions of privacy. *See supra* Section III. B.1. Because data privacy lacks a constitutional identity—or any singular identity—in U.S. law, it is murkier as to when the law ought to prioritize privacy over other interests. The point here is only to analogize to how antitrust has grappled with other incommensurate interests by considering the centrality and edges of data privacy and antitrust interests in their reconciliation.

400. *See supra* AREEDA & HOVENKAMP at 398.

401. See *supra* discussion of laws on biometric data at text accompanying footnotes 201–208.

Where a defendant's conduct is subject to both regulation and an antitrust claim, defendants have often argued that the specific regulatory scheme renders their actions immune from general antitrust law.[402] In analyzing such claims, courts will first consider whether there is express immunity from antitrust law in the regulatory statute. If there is not, courts will consider whether the regulatory regime is so pervasive as to imply a Congressional intent to immunize the regulated conduct from antitrust scrutiny—termed "implied immunity."[403]

Courts have long-established frameworks to assess claims of implied immunity in antitrust law. This law on implied immunity is useful in two respects for thinking about potential privacy immunity. First, this law may be applied directly as privacy takes on a more regulatory quality within U.S. law. The analytical framework on implied immunity originated where antitrust meets securities regulation,[404] but it has been applied across a variety of other regulatory contexts, as far afield as Medicaid regulation,[405] tax regulation by the Internal Revenue Service,[406] and natural gas regulation by the Federal Energy Regulatory Commission.[407] The Seventh Circuit confirmed in 2020 that "[i]mplied immunity is neither a securities doctrine nor a commodities doctrine. It is an antitrust doctrine. . . . The regulatory setting—securities, commodities, or something else—simply provides the backdrop against which the template is applied."[408]

This suggests the legal framework for implied immunity may also be applied by courts to privacy law as it takes on a more regulatory nature. Privacy law is

---

402. *See, e.g.,* Credit Suisse Sec. (USA) LLC v. Billing, 551 U.S. 264 (2007); Verizon Commc'ns Inc. v. Law Offs. of Curtis V. Trinko, L.L.P., 540 U.S. 398, 408 (2004); Samuel N. Weinstein, *Financial Regulation In The (Receding) Shadow of Antitrust*, 91 TEMP. L. REV. 447, 466–67 (2019) (examining twenty-six cases in which the defendant claimed antitrust immunity based on *Credit Suisse*).

403. *Credit Suisse*, 551 U.S. at 270–71 (explaining that some statutes expressly provide for immunity from antitrust law while others are silent and "Where regulatory statutes are silent in respect to antitrust, however, courts must determine whether, and in what respects, they implicitly preclude application of the antitrust laws.").

404. Id. at 270–76 (summarizing the Supreme Court precedents on implied antitrust immunity for securities regulation).

405. Horisons Unlimited v. Santa Cruz-Monterey-Merced Managed Med. Care Comm'n, No. 14-CV-00123, 2014 WL 3342565, at *10 (E.D. Cal., July 2, 2014) (applying *Credit Suisse* to find that a portion of the Medicaid regulatory scheme under the Social Security Act precludes the application of antitrust law to the claimed conduct).

406. Hinds Cnty., Miss. v. Wachovia Bank N.A., 700 F. Supp. 2d 378, 402 (S.D.N.Y. 2010) (applying *Credit Suisse* and concluding that the particular Internal Revenue Service regulations governing tax-exempt debt did not impliedly preclude application of the antitrust laws to the conduct).

407. Energy Mktg. Servs., Inc. v. Columbia Gas Transmission Corp., 639 F. Supp. 2d 643 (S.D. W. Va. 2009) (applying *Credit Suisse* and finding the Federal Energy Regulatory Commission's (FERC) regulatory oversight of sale and transportation of natural gas in interstate commerce did not conflict with antitrust laws therefore no immunity from antitrust for the alleged misconduct).

408. U.S. Futures Exch., L.L.C. v. Bd. of Trade of Chicago, 953 F.3d 955, 968 (7th Cir. 2020). While defendants are often less successful in actually obtaining implied immunity outside the securities context, the analytical framework is widely applied. Samuel N. Weinstein, *Financial Regulation In The (Receding) Shadow Of Antitrust*, 91 TEMP. L. REV. 447, 466–67 (2019) (examining twenty-six cases in which the defendant claimed antitrust immunity based on *Credit Suisse* but finding only five in which such immunity was successfully shown, almost all of which involved securities regulation).

proscribing more and more conduct that is and is not permitted,[409] including through novel rulemaking by the FTC and state privacy enforcers.[410] As this continues, it makes it more likely that, where both antitrust and privacy law apply, defendants will claim the pervasive data privacy regulation of their conduct implies immunity from antitrust law.

Second, the jurisprudence on implied immunity is also useful in a broader sense for courts, and even lawmakers and agencies, in thinking about countervailing privacy interests, because it has developed various approaches to defining conflicts between antitrust and other areas of law. Over time, cases on implied immunity have adopted different judicial definitions of what constitutes a "conflict." This variation offers a useful menu of potential options for defining conflicts where privacy regulation meets antitrust law, and how each approach would affect their interaction.

Courts begin the implied immunity analysis by trying to reconcile the regulatory scheme with antitrust laws whenever possible. Antitrust is repealed "only to the minimum extent necessary" to enable the regulation to work.[411] In defining when such immunity is truly necessary, the Supreme Court has articulated two different standards over time. The first, in older Supreme Court cases, required "clear repugnancy" between the regulation and antitrust law.[412] Leading cases like *Silver v. New York Stock Exchange* interpreted clear repugnancy to require a direct conflict between the regulation and antitrust before finding implied immunity.[413] This is assessed by looking at several factors, including the power of the particular regulatory agency to supervise the conduct at issue, whether the agency actually exercised that power, and the risk of a conflict if both antitrust and the relevant regulation are applied.[414] In this analysis, courts also consider how central the

---

409. *See supra* discussion in Part III. The Changing Character of U.S. Data Privacy Law and its Impacts on Antitrust Theory.

410. FED. TRADE COMM'N, FTC EXPLORES RULES CRACKING DOWN ON COMMERCIAL SURVEILLANCE AND LAX DATA SECURITY PRACTICES (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/S78V-5LR6]; California Privacy Protection Agency, Cal. Civ. Code §§ 7000–7304 (regulations adopted under California Privacy Rights Act in March 2023).

411. *Credit Suisse*, 551 U.S. at 271 (quoting *Silver v. N.Y. Stock Exch.*, 373 U.S. 341, 357 (1963)).

412. *Id.* at 275 ("This Court's prior decisions [referring to *Silver v. N.Y. Stock Exch.*, 373 U.S. 341 (1963), *Gordon v. New York Stock Exch., Inc.*, 422 U.S. 659 (1975), and *United States v. Nat'l Ass'n of Sec. Dealers, Inc.*, 422 U.S. 694 (1975)] also make clear that, when a court decides whether securities law precludes antitrust law, it is deciding whether, given context and likely consequences, there is a 'clear repugnancy' between the securities law and the antitrust complaint—or as we shall subsequently describe the matter, whether the two are 'clearly incompatible.'"); Nat'l Gerimedical Hosp. v. Blue Cross, 452 U.S. 378 (1981).

413. *Silver*, 373 U.S. at 357. *See also* on clear repugnancy Gordon v. New York Stock Exch., Inc., 422 U.S. 659 (1975); United States v. Nat'l Ass'n of Sec. Dealers, Inc., 422 U.S. 694, 729–30 (1975) (finding that the securities laws permit agreements prohibited by antitrust and "the antitrust laws must give way if the regulatory scheme established by the Investment Company Act is to work"); United States v. Nat'l Ass'n of Sec. Dealers, Inc. 422 U.S. 694 (1975).

414. *Credit Suisse*, 551 U.S. at 275–76 (synthesizing factors used to determine repugnancy in prior Supreme Court decisions regarding antitrust immunity for securities regulation, in addition to the possible "conflict" discussed above). The conclusion on whether the conduct is immune from antitrust

impugned practices are to the regulatory scheme and what it seeks to achieve.[415] Where no conflict is found, this standard means that both antitrust agencies and regulatory agencies are free to police the conduct.[416] Where there is a conflict, courts will infer a Congressional intent to imply antitrust immunity.

A second approach to implied immunity appears in a more recent Supreme Court decision on the topic, *Credit Suisse Securities (USA) LLC v. Billing*.[417] The case softens the test for implied immunity to require only a risk of potential inconsistency between the regulation and antitrust law, rather than an extant conflict. *Credit Suisse* involved claims that the defendants had violated both securities laws as overseen by the Securities and Exchange Commission (SEC) and also Section 1 of the Sherman Act, by jointly setting securities prices.[418] The defendants successfully argued that the securities regulatory scheme rendered their conduct impliedly immune from antitrust scrutiny.[419]

The Court reasoned that even if antitrust applied only when it is *consistent* with securities law—meaning when there is no direct or actual conflict (as was true on the facts of *Credit Suisse*)—antitrust courts might make errors in determining which conduct securities law permits or prohibits because that securities analysis requires complex evidentiary and legal line drawing.[420] Based on this risk that antitrust courts might reach different conclusions from the SEC on the permissibility of conduct, the Court worried that antitrust decisions could interfere with the efficient regulation of securities markets.[421] The SEC needed to be able to make securities regulatory judgments "free from the disruption of conflicting judgments that might

---

depends heavily on the specifics of the regulatory scheme and antitrust conduct at issue in each case. *Id.* at 271("Determining whether implied antitrust immunity applies 'may vary from statute to statute, depending upon the relation between the antitrust laws and the regulatory program set forth in the particular statute, and the relation of the specific conduct at issue to both sets of laws.'"). Even within the securities context where this thinking originates, the ultimate findings on implied immunity vary with the specifics of the statutory provision and the conduct. *Compare id.* at 285 (finding implied immunity from Sherman Act claims based on Securities and Exchange Commission (SEC) regulatory authority over underwriting syndicates for initial public offerings) and *Gordon*, 422 U.S. at 690 (finding antitrust law in conflict with SEC power to regulate the mechanism for determining securities exchange commissions) *with Silver*, 373 U.S. at 357 (finding no antitrust implied immunity where a securities exchange ordered members to eliminate telephone connections with nonmembers, as the Securities and Exchange Commission had no jurisdiction to review particular instances of the applications of rules enacted by exchanges—despite a broader authority to request changes in the rules themselves).

415. *Credit Suisse*, 551 U.S. at 275–76.

416. *See, e.g.*, Otter Tail Power v. United States, 410 U.S. 366, 372–75 (1973).

417. *Credit Suisse*, 551 U.S. at 270–76 (summarizing the Supreme Court precedents on implied antitrust immunity for securities regulation).

418. *Id.* at 269–70. Section 1 of the Sherman Act prohibits contracts, combinations, and conspiracies in restraint of trade. *See* 15 U.S.C. § 1.

419. *Credit Suisse*, 551 U.S. at 278–79.

420. *Id.* at 279–83 (finding an "unusually serious legal line drawing problem" in determining lawful and unlawful conduct in securities law and concluding there is a substantial risk of harm to securities markets from the intervention of antitrust litigation that results).

421. The Securities and Exchange Commission is the primary federal securities regulator.

be voiced by courts exercising jurisdiction under the antitrust laws."[422] While *Credit Suisse* continued to use the same terminology of "clear repugnancy," in effect this expanded the concept beyond the earlier cases like *Silver v. New York Stock Exchange*. Under *Credit Suisse*, clear repugnancy and thus implied immunity from antitrust law can be found even in instances of no actual conflict with a regulation but rather a risk of inconsistent antitrust judgments arising from judicial error.[423]

This experience in defining regulatory conflicts illustrates two potential approaches that antitrust could adopt in defining conflict with countervailing privacy regulations. It could adopt a standard of true or actual conflict, as existed in the law prior to *Credit Suisse* in cases like *Silver v. New York Stock Exchange*. This approach would leave a greater scope for the application of antitrust law alongside privacy regulation. Both would apply as complements, with antitrust precluded only where there is an actual conflict with privacy law. Or, instead, antitrust could adopt a standard like that in *Credit Suisse*, finding a "conflict" where there is merely a risk of inconsistent judgments between antitrust and privacy regulation. This would leave greater scope for privacy regulation, and regulators, to operate free from potentially inconsistent conclusions in antitrust law.

This choice of legal standard will need to be informed by broader Congressional policy decisions on when, and to what extent, to prioritize privacy or competition. The point here is that antitrust law is not adrift in formulating more nuanced approaches to analyzing privacy law tensions and conflicts, as it has done so with other regulation and can usefully draw on that experience.

Regardless of the blackletter law that ultimately emerges in this space, the broad takeaway is that all of this proposed analysis is new to how antitrust conceives of privacy. The analysis in this Section moves beyond the treatment of privacy as a factor in competition. Privacy-as-quality theory, while still useful, offers no answer on how antitrust can better understand the different identities of privacy within law, how to analyze privacy pretext, or how to begin defining theories of conflicts and exceptions between the two areas of law. These issues are not about the quality-based effects on privacy competition and consumer welfare within the standards of antitrust law. Rather, they are about how antitrust law begins to approach data privacy as its own area of doctrine, one that includes rights and regulation that may, at times, be at odds with antitrust law and the interests it protects.

CONCLUSION

This Article argues that antitrust law has yet to understand data privacy in a

---

422. *See* United States v. Nat'l Ass'n of Sec. Dealers, Inc., 422 U.S. 694, 734 (1975); *see also* Gordon v. New York Stock Exch., Inc., 422 U.S. 659, 681 (1975) (finding implied immunity from antitrust law for certain regulated conduct in the resale of mutual fund securities where the Securities and Exchange Commission chose to require only disclosure and self-regulation to control that conduct, rather than engaging in rulemaking it was empowered to pursue under the applicable securities law).

423. *Credit Suisse*, 551 U.S. at 264 (explaining conflict includes a "risk of . . . conflicting guidance, requirements, duties, privileges, or standards of conduct").

meaningful way. Antitrust agency, scholarly, and judicial treatment of privacy has been monolithic, treating privacy exclusively as a parameter of product quality. This unitary conception of data privacy is causing courts and lawmakers to prioritize competition interests over privacy, without clear justification. There is also a risk this unexamined competition primacy will redound to privacy law itself, weakening the legal recognition of privacy harms.

Existing antitrust theory remains useful at times, but does not account for newer conceptions of data privacy in law. In particular, the Article explores two paradigm shifts occurring in U.S. data privacy law—the move away from notice and consent toward prohibitions and duties, and the proliferation of privacy rights. It argues that these seismic changes will press antitrust toward more pluralistic thinking about data privacy, because each creates new variability in the interactions between these areas of law. Portions of data privacy law are beginning to revisit—and resist—the previously-shared assumption with antitrust law that individuals benefit from competition for the sale of their personal data.

The Article then looks ahead to how antitrust can develop more nuanced conceptions of what privacy is to antitrust law. While acknowledging that current theory will remains relevant at times, it calls for antitrust institutions to build their privacy competency and collaboration, to grapple more deeply with the scope and nature of protected interests in privacy law. Where privacy law is at odds with antitrust, the Article examines how legislatures and courts can begin to think about exceptions, immunities, and conflicts in antitrust law for data privacy, by drawing on antitrust theories of other incommensurate interests protected by regulation, patent, and free speech law. With these new analytical approaches, the Article seeks to expand the notions of what data privacy is to antitrust law, and to better account for the rich and variable interactions emerging between the two.