THE YALE LAW JOURNAL FORUM

JANUARY 18, 2021

The New Antitrust/Data Privacy Law Interface

Erika M. Douglas

ABSTRACT. Antitrust theory portrays data privacy as a factor, like quality, that improves with competition. This Essay argues that view is an incomplete account of the new interface between antitrust and data privacy. The more complex reality is that, over the last twenty-five years, data privacy has also become a separate area of legal doctrine. In that capacity, data privacy law may clash at the margins with antitrust—much like intellectual property or consumer protection law did before it. The Essay sheds new light on this tension at the interface of antitrust and data privacy. It provides a descriptive, historical and comparative account of the friction emerging between these areas of law in the digital economy, where data access can both drive competition and reduce privacy. The Essay then lays out a new approach to analyze claims of conflicting data privacy and competition interests, one that emphasizes the accommodation of both areas of law.

INTRODUCTION

Antitrust law and data privacy law are powerful forces shaping the treatment of digital information. Both are converging on the companies that hold and use our data—digital platforms like Facebook, Google, Apple and Amazon.[1] These entities are perennial favorites of Federal Trade Commission (FTC) data privacy

1. The term "digital platform" is used here to mean large technology companies whose major services create value by intermediating between different online groups. *See, e.g.*, Ohio v. Am. Express Co., 138 S. Ct. 2274, 2280 (discussing two-sided platforms).

enforcement,[2] and of the strict new European data protection regime.[3] At the same time, these digital giants face antitrust scrutiny from federal and state antitrust authorities,[4] both Houses of Congress,[5] and international competition law enforcers[6] for their data-driven competition practices.

---

2. As discussed further below, section 5 of the FTC Act empowers the FTC to prevent unfair or deceptive acts or practices, and that power forms the basis for U.S. data privacy protection outside of sector-specific privacy laws. 15 U.S.C. § 45(a)(1) (2018); *see, e.g.*, Agreement Containing Consent Order at 5-8, *In re* Facebook, Inc., No. 092 3184, (F.T.C. 2011); Order Modifying Consent Order, *In re* Facebook, Inc., No. C-4365 (F.T.C. Apr. 27, 2020), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/6S9P-A3QS]; Complaint for Civil Penalties and Other Relief at 9, United States v. Google, Inc., 2012 WL 5833994 (N.D. Cal. Nov. 20, 2012) (No. CV 12-04177 HRL) (alleging that Google misled its users into thinking that it would not collect or use information about their web browsing activity); Complaint, *In re* Twitter, Inc., 2010 WL 2638509 (F.T.C. 2010) (No. C-4316) (alleging that Twitter deceived its customers when it failed to honor user choices to designate certain "tweets" as private).

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

4. The Department of Justice (DOJ) and the Federal Trade Commission (FTC) enforce U.S. federal antitrust law. *See, e.g.*, Press Release, Dep't of Justice, Justice Department Sues Monopolist Google for Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws [https://perma.cc/ZCT2-G868] (claim initially including eleven state Attorneys General); Press Release, Fed. Trade Comm'n, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology [https://perma.cc/RB5V-7P2X]; Press Release, Dep't of Justice, Justice Department Reviewing the Practices of Market-Leading Online Platforms (July 23, 2018), https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online-platforms [https://perma.cc/G2Z6-EGZG]; Complaint, Colorado et al. v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020), https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf [https://perma.cc/JQ7F-AFNL]; Complaint, Texas et al. v. Google, No. 4:20-cv-00957-SDJ (E.D. Tex. Dec. 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216_1%20Complaint%20(Redacted).pdf [https://perma.cc/QD3C-HWFE].

5. *See, e.g.*, H. COMM. ON THE JUDICIARY, SUBCOMM. ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REP. AND RECOMMENDATIONS (2020), https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf [https://perma.cc/QG37-8SZW] [hereinafter HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS]; *Understanding the Digital Advertising Ecosystem and the Impact of Data Privacy and Competition Policy*: *Hearing Before the S. Comm. on the Judiciary*, 116th Cong. (2019).

6. *See, e.g.*, DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, DISINFORMATION AND 'FAKE NEWS': FINAL REPORT, 2017-19, HC 1791, at 38 (UK) (discussing how Facebook denied competitors, such as the company Vine, access to data); Press Release, Antitrust: Commission Opens Investigations into Apple's App Store Rules (June 16, 2020), https://ec.europa.eu

We are only beginning to theorize this new convergence of digital data privacy and antitrust law. This Essay argues that, so far, our understanding of the new antitrust/data privacy law interface is incomplete. It provides a descriptive, historical and comparative account of the tension appearing between antitrust and data privacy law, which has been overlooked by existing theories.

Part I explains why this intersection of law is new, then describes the two main theories on the antitrust/data privacy law interface. One insists on doctrinal separation between these areas of law, and the other treats privacy as an element of quality in antitrust analysis. Both theories emphasize complementarity between privacy and competition.

Part II argues that these theories are incomplete in two related ways. First, the interests of data privacy and antitrust law are not always complementary — they can be in tension, proof of which is developed throughout this Essay. Competition may be enhanced by data access, while data privacy is eroded by it. Second, and relatedly, these theories ignore the interaction of antitrust with data privacy law as a separate, and potentially opposing, area of new legal doctrine — not merely as a factor within antitrust analysis.

The recent Ninth Circuit decision, *HiQ v. LinkedIn*, provides an example of this new tension.[7] LinkedIn terminated HiQ's access to user profile data on the LinkedIn social network. LinkedIn argued that HiQ violated user privacy settings through its collection and dissemination of profile data in data analytics

/commission/presscorner/detail/en/ip_20_1073 [https://perma.cc/UA27-ZCPB] (investigating "whether Apple's rules for app developers on the distribution of apps via the Apple Store violate EU competition rules"); Press Release, Antitrust: Commission Opens Investigation into Possible Anti-Competitive Conduct of Amazon (July 17, 2019), https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291 [https://perma.cc/LWV3-HGJW] (investigating Amazon's use of "sensitive data from independent retailers who sell on its marketplace"). The European competition authorities have fined Google three times in recent years for abuse of monopoly. *See* Press Release, Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising (Mar. 20, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770 [https://perma.cc/X6SM-3VQZ] (fining Google for its contracting practices in online advertising); Press Release, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 17, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 [https://perma.cc/H5VD-X52P] (fining Google for preferring its own websites in search results); Press Release, Antitrust: Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine (July 18, 2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581 [https://perma.cc/A5YT-RZAL] (fining Google for restrictions imposed on Android device manufacturers and mobile network operators related use of Google Search).

7. 938 F.3d 985 (9th Cir. 2019). The case involved state unfair competition law claims, but raises arguments similar to those canvassed here for federal antitrust law.

software.[8] HiQ argued the termination was, in fact, unfair competition—that HiQ competed with LinkedIn to supply such software, and LinkedIn selectively banned it to eliminate a rival.[9] The Ninth Circuit upheld a preliminary injunction that granted HiQ continued access to LinkedIn user profile information.[10] This effectively guaranteed that HiQ could continue to override user privacy settings, in the name of competition.[11] The Ninth Circuit remedy is difficult to reconcile with the FTC's privacy law enforcement against other digital platforms for their failure to honor user privacy settings—settings much like those disregarded by HiQ.[12]

Part III of this Essay offers a foundational shift in thinking about the new antitrust/data privacy interface. It paints a picture of the emerging tension between antitrust and data privacy law, first with specific examples where data privacy and competition are facing off on digital platforms. It then contextualizes the tension, situating it within the history of consumer protection law and the comparative European legal landscape. Both perspectives suggest an impending clash between data privacy and antitrust law. This Part concludes with an early-stage observation: faced with tradeoffs between competition and privacy, the tendency of theoretical, institutional and evidentiary biases will likely be to prefer competition—as occurred in the *HiQ v. LinkedIn* case.

Part IV proposes the first analytical framework to address tension between antitrust and data privacy law. When there are claims of legitimate, but conflicting, data privacy and competition interests, the proposal treats both doctrines as relevant to determining the scope of permitted conduct. Neither antitrust law nor data privacy law is presumed to have primacy. Instead, the importance of the

---

8. *HiQ*, 938 F.3d at 994-995 (discussing user privacy interests protected by the "Do Not Broadcast" setting on LinkedIn).

9. *Id*. (discussing HiQ's arguments to this effect at the District Court).

10. *Id.* at 1005. The Ninth Circuit was skeptical of LinkedIn's evidence that users invoked the privacy settings in order to prevent dissemination of profile changes, noting the settings could be engaged for reasons other than privacy.

11. *Id.* at 994-95 (expressing skepticism that users have privacy interests in controlling public profile data, finding balance of hardships tips heavily in HiQ's favor given HiQ's interest in continuing its commercial operations).

12. *See, e.g.*, Complaint for Civil Penalties and Other Relief at 9, United States v. Google, Inc., No. CV 12-04177 HRL (N.D. Cal. Aug. 8, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf [https://perma.cc/32ZH-E4HP] (considering user privacy settings on Google's Chrome web browser; arguing Google inaccurately represented to users whether its browser was tracking their online activity through cookies, a digital tracking technology); Agreement Containing Consent Order, Facebook, Inc., No. 092 3184, (F.T.C. Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/YSM5-G3VB] (finding Facebook deceived users regarding the control over their data conferred by privacy settings on the social media service).

interests at stake are evaluated with reference to each area of law. This proposal is modeled on theory from other, more established doctrinal intersections with antitrust law, such as patent and consumer protection law.

I. EXISTING THEORIES ON THE ANTITRUST/DATA PRIVACY INTERFACE

This Part provides a short history to illustrate why the interaction between antitrust law and data privacy is new. It then explains the two most commonly articulated, but opposing, theories on the antitrust/data privacy interface. Lastly, it describes the tendency of both theories to emphasize complementarity between these two areas of law.

These theories are new, as the intersection of law is itself quite new. It is only in the last twenty-five years that the FTC has established the "new common law of privacy."[13] The rise of the agency as the *de facto* federal data privacy regulator occurred in lockstep with the emergence of the internet, from the mid-1990s to the present.[14] Individuals were suddenly engaging in a myriad of new electronic activity, placing their data online in ever-growing amounts. Spotty, sector-specific privacy legislation left large swathes of that new online activity unprotected by any data privacy laws.[15] Congress urged the FTC to fill these gaps, which the agency did using its general consumer protection authority under section 5 of

---

13. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598-600 (2014) (describing and labelling the emergence of 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). The principles shaping the FTC's approach can be traced back to the Fair Information Privacy Practices (FIPPS), an influential statement of basic protections for handling personal data. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, NO. (OS)73-94, REPORT: RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 50 (1973) [hereinafter DEP'T OF HEALTH, EDUC. & WELFARE REPORT], https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/N8LY-X9GS] (providing the first articulation of the FIPPS).

14. *See* 15 U.S.C. § 45(a)(1) (2018); *Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 2 (2010) (statement of Jon Leibowitz, Chairman, FTC) (describing FTC enforcement of data privacy emerging alongside the internet). Though the FTC enforced the Fair Credit Reporting Act from the 1970s onwards, the expansion of the agency's privacy enforcement under section 5 FTC Act, and its other statutory data privacy powers, did not begin until around 1995. Solove & Hartzog, *supra* note 13, at 598-99.

15. Solove & Hartzog, *supra* note 13, at 587 (canvassing sectoral privacy legislation and observing its application only to certain types of data and certain entities). Even now, U.S. consumers have no omnibus right to control their data, and the sectoral legislation does not apply to much of the data collection and use by digital platforms. *Id.*

the FTC Act. Section 5 empowers the FTC to prevent unfair or deceptive acts or practices in the marketplace.[16] The FTC began to police companies' false or misleading promises regarding the collection, use, and sale of consumers' personal data. Over time, these efforts expanded and developed into a body of standards that seek to protect consumers' reasonable expectations of privacy. An early internet company was among the FTC's first enforcement targets,[17] and the agency has continued to focus on digital companies and their privacy practices ever since.

The novelty of the interface between antitrust law and data privacy is best illustrated in the context of monopoly enforcement.[18] Consider that the rise of data privacy law coincides precisely with a twenty-year absence of monopolization enforcement by U.S. antitrust agencies. Around the time data privacy law began to take hold, "the anti-monopoly provisions of the Sherman Act went into a deep freeze from which they have never really recovered."[19] The last significant government anti-monopoly case ended around 2001.[20] Monopolization enforcement has unthawed only very recently, with a case filed against Google in late

16. 15 U.S.C. § 45(a)(1) (2018). The FTC brings most of its data privacy cases under the "decepti[on]" branch of section 5 of the FTC Act, which has been interpreted to prohibit misrepresentations, omissions or other practices that mislead a consumer acting reasonably in the circumstances, to the consumer's detriment. 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* Solove & Hartzog, *supra* note 13, at 598-99.

17. *See, e.g.*, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case*, FED. TRADE COMMISSION (Aug. 13, 1998), https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting [https://perma.cc/3TAJ-QRCY] (describing an FTC data privacy enforcement action against GeoCities, an early social networking site).

18. In merger review, there is a slightly longer history of considering the interaction between antitrust law and data privacy, beginning around 2007 with the FTC's analysis in the *Google/Doubleclick* merger. *See* Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, at 2 (F.T.C. Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [https://perma.cc/8N4T-W4ST]. Some of that thinking has extended to the monopolization context and is discussed here. However, the theories around data privacy are far from complete or fully settled in any area of antitrust law.

19. TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 108 (2018).

20. *See* United States v. Microsoft Corp., 253 F.3d 34, 45-47 (D.C. Cir. 2001). This Department of Justice Antitrust Division case long held the distinction as the last significant section 2 Sherman Act case, *see* 15 U.S.C. § 2 (2018), at least until the filing against Google, which occurred during the drafting of this Essay, *see* Complaint, *United States v. Google LLC*, No. 1:20-CV-03010 (D.D.C. Oct. 20, 2020). The DOJ pursued Microsoft for exclusionary misconduct, including technical tying, exclusion of competitors from distribution channels, and other conduct, which Microsoft engaged in to protect its Windows operating system monopoly from

2020.[21] This coincidence of timing—quiet in anti-monopolization enforcement while data privacy law bloomed—means that these areas of law are only now beginning to coexist in American law. The theories of their interaction are thus new, and still developing.

A. Existing Theories: Separatist and Integrationist Views

The first theory on this legal interface casts data privacy as beyond the purview of antitrust law.[22] This "separatist" perspective emphasizes the historical and doctrinal separation between the FTC's competition mandate and its consumer protection mandate.[23] It advocates for the continued delineation between data privacy (which is rooted in the consumer protection mandate) and antitrust law. Separatist theory views each of these areas of law as protecting against distinct legal harms. Antitrust law is seen as best suited to address conduct harmful to overall consumer welfare or economic efficiency in the marketplace.[24] Data privacy law, in contrast, is seen as a better fit for ensuring that individual consumers receive the benefit of their bargains, given its focus on informed choice and reasonable consumer expectations.[25] The central concern of separatists is that the incorporation of privacy considerations into antitrust analysis will create confusion in the application of antitrust law's consumer welfare standard.[26]

---

the rise of competing internet browsers. *See Microsoft Corp.*, 253 F.3d at 47. Private parties continue to bring litigation, but such cases lack the power and significance of government anti-monopoly enforcement, and certainly do not threaten the same likelihood of success.

21. Complaint, *United States v. Google LLC*, No. 1:20-CV-03010 (D.D.C. Oct. 20, 2020); *see also* Complaint for Injunctive and other Equitable Relief, F.T.C. v. Facebook, Inc., (D.D.C. Dec. 9, 2020), https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf [https://perma.cc/25SM-5Q7J].

22. *See, e.g.*, James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1146 (2013) (concluding that "antitrust is the wrong vehicle to address privacy concerns"); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 138-43 (2015).

23. *See* Ohlhausen & Okuliar, *supra* note 22, at 138-43. The FTC initially had only the power to enforce a competition law mandate. Later, with the passage of the Wheeler-Lea Act, Congress granted the FTC its separate consumer protection authority. 15 U.S.C. § 45(a)(1) (2018) (providing the FTC with consumer protection powers).

24. *See* Ohlhausen & Okuliar, *supra* note 22, at 154-55.

25. *Id*.

26. *Id*. 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."); *see* 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)).

The second widely articulated view on the interface between antitrust and data privacy posits that antitrust analysis ought to consider data privacy whenever it is an element of quality-based competition. This "integrationist" approach incorporates data privacy into longstanding antitrust analytical frameworks.[27] It starts from the well-established position that consumer welfare is improved by competition that is based not only on price, but also on non-price factors, like quality.[28] It then interprets the concept of "quality" broadly, to encompass privacy-based competition.

When the facts indicate that "[c]ompanies compete to offer more or less privacy to users,"[29] the integrationist view considers whether mergers or misconduct are likely to impact that privacy-based competition. For example, consider two internet browser companies who seek to merge. If, pre-merger, those companies compete to offer consumers better online privacy protection, then their combination could reduce the privacy options available to consumers in the market post-merger. Integrationist theory would consider that reduction in privacy-as-quality in its assessment of whether the merger will substantially reduce competition. If, instead, there was no privacy-based competition between the merging parties, then integrationist theory would deem any privacy concerns related to the merger to be beyond the purview of antitrust law.[30]

---

27. Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 2, 25-26 (2020).

28. Nat'l Soc'y of Prof'l 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.").

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

30. *See, e.g.*, Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, at 2 (F.T.C. Dec. 20, 2007) [hereinafter Statement of FTC Concerning Google/DoubleClick], https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [https://perma.cc/8N4T-W4ST] (noting limits of FTC jurisdiction in declining to consider privacy when unrelated to quality-based competition).

To date, integrationist theory is the most developed and accepted view on the interaction between antitrust law and data privacy.[31] The FTC,[32] DOJ,[33] and European competition authorities[34] have adopted this integrated view and have applied it in merger cases. Several scholars have also expressed support for integrationist theory.[35]

B. Existing Theories Emphasize Complementarity

Under both the separatist and integrationist theories, agencies and scholars have tended to emphasize complementarity between antitrust and data privacy

---

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

32. *See* Statement of Federal Trade Commission Concerning Google/DoubleClick, *supra* note 30, at 2-3; Deborah Feinstein, FTC Bureau of Competition, *The Not-So-Big News About Big Data*, Competition Matters Blog (June 16, 2015), https://www.ftc.gov/news-events/blogs/competition-matters/2015/06/not-so-big-news-about-big-data [https://perma.cc/T8W2-R9XP] ("[T]he FTC has explicitly recognized that privacy can be a non-price dimension of competition.").

33. Makan Delrahim, Assistant Attorney Gen., Dep't of Justice, Remarks for the Antitrust New Frontiers Conference: ". . . And Justice for All": Antitrust Enforcement and Digital Gatekeepers (June 11, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers [https://perma.cc/8UM9-FBGA] ("[D]iminished quality is also a type of harm to competition. . . . [P]rivacy can be an important dimension of quality.").

34. Margrethe Vestager, Comm'r for Competition, Eur. Comm'n, Mackenzie Stuart Lecture at Cambridge: Making the Data Revolution Work for Us (Feb. 4, 2019), https://wayback.archive-it.org/12090/20191129203859/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-revolution-work-us_en [https://perma.cc/5SJ7-ACBK] ("[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); Press Release, Eur. Comm'n, 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/Q9RB-WBA5] (same).

35. *See, e.g.*, Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets,* 76 ANTITRUST L.J. 769, 773 (2010) ("[P]rivacy is an increasingly important dimension of competition as well, which is exactly why modern antitrust analysis must take privacy into account."); Robert H. Lande, *The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern*, *in* FTC: WATCH, at 1 (Wash. Regulatory Reporting Assocs. No. 714, 2008); Maurice E. Stucke & Allen P. Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, ANTITRUST SOURCE, Apr. 2015, at 1, 4 ("Privacy has been recognized as a non-price dimension of competition in the sense that firms can compete to offer greater or lesser degrees of privacy protection.").

interests. Separatist theory casts these areas of law as puzzle pieces, "complementary [in] nature," but not overlapping.[36] In the same vein, the typical example used to describe integrationist theory is a merger analysis that casts data privacy as correlated with competition. As in the browser example above, integrationist theory considers whether a transaction is likely to lessen pressure on the merging firms to compete based on privacy, resulting in fewer privacy-protective product options for consumers post-merger.[37] This reflects a relationship where competition drives privacy, and when one declines, so does the other. Recent characterizations of digital market power and abuse of dominance similarly link the decline of competition with the erosion of data privacy.[38]

Policy discussions reflect this same complementarity narrative. A favorite example of antitrust agencies is the presumed positive effect of data portability rights on competition.[39] Data privacy laws around the world have begun to grant consumers the right to move their digital data from one online service provider to another, referred to as "data portability."[40] Antitrust agencies often point to such data portability rights as positive for competition.[41] In the absence of portability, the thinking is that consumers may hesitate to switch to a competing

---

36. *See* Ohlhausen & Okuliar, *supra* note 22, at 138.

37. *See* Statement of Federal Trade Commission Concerning Google/DoubleClick, *supra* note 30, at 2.

38. *See, e.g.*, HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 5, at 43 ("[A] dominant platform can use its market power to extract more data from users, undermining their privacy."); *id*. at 52 ("The best evidence of platform market power therefore is not prices charged but rather the degree to which platforms have eroded consumer privacy without prompting a response from the market."); *see also* Dig. Competition Expert Panel, *Unlocking Digital Competition*, U.K. DEPARTMENT OF THE TREASURY 43 ¶ 1.128 (2019) ("[T]he misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by a lack of competition. It may also be a method for achieving and cementing market power.")[hereinafter, U.K. Digital Competition Expert Panel].

39. Data portability is the ability to copy, move or transfer data. *See* 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/77CS-AFDD] ("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, Comm'r for Competition, European Comm'n, Remarks at the Privacy Platform Event: Competition and Privacy in Markets of Data (Nov. 26, 2012), http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm [https://perma.cc/F777-6NJH] ("[P]ortability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them.").

40. *See, e.g.*, GDPR, *supra* note 3, at art. 20 (requiring data portability for personal data between data controllers); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100(d) (West 2020) (requiring personal information be provided in a portable format upon request).

41. *See* sources cited *supra* note 39.

digital service because that would mean leaving their data behind on the old service. When consumers are empowered to port their data, the assumption is that this encourages consumers to switch to new services, which fuels new entry and digital competition.

If this prevailing narrative of complementarity always holds true, that is incredibly convenient for the enforcement of both antitrust and data privacy law against the same digital platforms. It creates a cohesive legal landscape, in which each doctrinal area can pursue its respective enforcement goals without any question of which to prefer.

As the next Part of this Essay argues, however, the assumption of complementarity is unlikely to hold in every interaction between competition and data privacy, particularly in the digital economy. It is a largely unexamined assumption, made as part of emerging theories on this new intersection of law.

II. ACKNOWLEDGING NON-COMPLEMENTARITY: DATA PRIVACY LAW AS A DISTINCT AND OPPOSING LEGAL DOCTRINE

What if instead of complementarity, there was a negative correlation between competition and data privacy—what if more competition could result in less privacy (or vice versa)? Varying the scenarios above, what if the merger instead combined two digital advertising firms, and the result was less competition to collect and use consumer data for targeted ads? What if, in exercising their data portability rights, consumers instead chose to port their data in the opposite direction, from new entrants to the incumbent digital platforms that offer larger networks?[42] Data portability could cement monopolies rather than promote competition.

This non-complementarity creates two challenges for antitrust analysis. First, it raises a variation on the familiar question of how to evaluate tradeoffs between different dimensions of product quality.[43] Product design changes may cause privacy to decrease, but at the same time, improve other elements of product quality. How does antitrust analysis evaluate the effects on consumer welfare

42. 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 firm with more (other) users.

43. *See* Manne & Sperry, *supra* note 31 at 5-6 (discussing the challenge of analyzing tradeoffs between privacy and other elements of product quality; providing the example of trading data privacy for more accurate search results or more accurately targeted advertising).

when there are multiple different dimension of quality? Antitrust has faced similar questions before in its evaluation of non-price effects, albeit outside of the privacy context.[44]

Second, non-complementarity raises the problem of antitrust law and data privacy law pursuing opposing interests. Data privacy does not exist only as an element of quality within antitrust analysis. Data privacy law is also a distinct area of doctrine that, at times, pursues interest at odds with the antitrust goal of promoting competition. In that sense, data privacy law is much like intellectual property or consumer protection law. The difference is that, while we have long examined these other interfaces with antitrust law,[45] we have scarcely begun to consider the equivalent interaction with data privacy law. The remainder of this Essay addresses this second dilemma, because it is novel and it is not addressed by existing theories.

Separatist and integrationist theories both lack an explanation of how antitrust law interacts with data privacy law in its capacity as a distinct area of legal doctrine. Though separatist theory acknowledges privacy as a distinct area of law, it assumes away any interaction by insisting that antitrust and data privacy are separate. But, the fact that two areas of law are doctrinally separate does not preclude their meeting. Separate doctrinal areas of law often interact with antitrust law. It is correct to say, for example, that antitrust law and patent law are historically and doctrinally separate, but equally correct to observe the significant judicial and scholarly thought devoted to their interaction. Likewise, antitrust law and consumer protection law are separate in U.S. legal doctrine, but interact at their edges.[46] The same is now true for data privacy law and antitrust law.

Integrationist theory leaves a similar gap. When there is no privacy-as-quality competition, integrationist theory dismisses data privacy as outside the ambit of antitrust analysis. In fact, data privacy may remain highly relevant, as a separate area of law that seeks disparate treatment of consumer data and reduces competition.

The central disagreement between the two existing theories is whether data privacy is properly considered a factor in antitrust analysis. This is a valid question. However, it is not the only question at this intersection of law. Regardless of whether or not data privacy is integrated into antitrust analysis as a quality-type factor, it remains true that these two areas of law may intersect.

---

44. *See, e.g.*, Berkey Photo, Inc. v. Eastman Kodak Co. 603 F.2d 263, 286-87 (2d Cir. 1979), *cert. denied*, 444 U.S. 1093 (1980) (deferring to consumer choice to evaluate tradeoffs in camera design features, such as portability and film shelf life).

45. *See, e.g.*, Mark A. Lemley, *A New Balance Between IP and Antitrust*, 13 SW. J.L. & TRADE AM. 237, 245 n.25 (2007) (noting "voluminous literature on the overlap" between patent law and antitrust law).

46. *See* discussion *infra* Section III.B.1.

To be clear, this is not an argument that there is a hard conflict of law wherein antitrust law requires action that privacy law prohibits (or vice versa).[47] Rather, it is a contention that these two areas of law are increasingly interacting, and, at times, that they pursue opposing interests.

In the digital economy, this potential for antitrust and data privacy to pursue opposing interests is particularly apparent. From an antitrust perspective, consumer data plays an undeniably significant role in digital competition. Leading digital platforms rely on collection and analysis of masses of data about consumers to drive their services, like search and social media—and to drive their profits as well.[48] The companies that collect and monetize digital data in the smartest ways win the race to compete, attracting users, and benefit from the network effects that characterize many of these online services. New theories of anti-competitive harm focus on this data-driven competition, and the power gained by digital platforms through their control and accumulation of data.[49]

---

47. Though theoretically possible such a conflict could occur, it seems implausible that one agency (or two separate Bureaus, in the FTC's case) would pursue a defendant for a violation of one area of law where the conduct was compelled under a different area of law by the other agency. Former FTC Commissioner Thomas B. Leary noted a similar theoretical possibility at the broader consumer protection/antitrust law interface. *Leary: Consumer Protection-Antitrust Conflict*, FTC (Feb. 9, 2004), https://www.mlexwatch.com/articles/205/print?section=ftcwatch [https://perma.cc/PV95-4WMV] (quoting FTC Commissioner Thomas B. Leary's statement that "at least theoretically, cases in which a professional standard or an ethical code of conduct might be encouraged by the FTC's Consumer Protection staff but run afoul of its Antitrust staff"). The FTC Bureau of Consumer Protection has jurisdiction over data privacy and data security cases, while the FTC's Bureau of Competition has jurisdiction over competition cases, as does the Department of Justice Antitrust Division.

48. *See* Ohlhausen & Okuliar, *supra* note 22, at 130, 132 ("The value and importance of consumer data to e-commerce and the Internet ecosystem is widely understood."). In the last minute alone, Google fielded over four million user searches. *Data Never Sleeps 7.0*, DOMO, INC., https://www.domo.com/learn/data-never-sleeps-7 [https://perma.cc/M2ZY-37JX] (reporting an average 4,497,420 Google searches per minute in 2019); Facebook users uploaded almost 150,000 photos. *Data Never Sleeps 8.0*, DOMO, INC., https://www.domo.com/learn/data-never-sleeps-8 [https://perma.cc/28X8-LFTC] (reporting that in 2020 to date, an average of 147,000 photos were uploaded to Facebook per minute); Amazon sold up to 81,000 products, marketed through data-driven algorithms. *Data Never Sleeps 8.0*, DOMO, INC., https://www.domo.com/learn/data-never-sleeps-8 [https://perma.cc/28X8-LFTC] (reporting that in 2020 to date, an average of 147,000 photos were uploaded to Facebook per minute).

49. *See, e.g.*, MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 277 (2016); Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1679 (2013) (arguing that the accumulation of data by incumbent monopolists is a "strategic asset" that acts as a barrier to entry, foreclosing competition); EUR. DATA PROT. SUPERVISOR, PRIVACY AND COMPETITIVENESS IN THE AGE OF BIG DATA 30–31 (2014) (describing scholarship theorizing that "[p]owerful or dominant undertakings are able to . . . create barriers to entry through their control of huge personal datasets . . . [that] could prevent the development of competing products"). However, these arguments rest on the

From a data privacy perspective, much of that same information is personally identifiable and thus limited in its collection, use, and sale by the FTC's new common law of data privacy. The FTC's enforcement of section 5 has long been directed at internet companies, including the digital platforms that collect and use our data to compete.

When privacy law restricts the collection and use of information, that creates potential tradeoffs with the benefits of data-driven competition. For example, Catherine Tucker observes that increased privacy regulation decreases data sharing between firms, which she predicts will reduce competition in online advertising.[50] Early research on the General Data Protection Regulation (GDPR), a tough new European data privacy protection law, suggests that improved consumer control over personal data may also reduce competition in consumer data-intensive markets, because it limits data sharing.[51] The FTC itself has begun to recognize this tradeoff between data competition and privacy.[52]

Enforcers, courts and digital platforms are left with two opposing legal pressures on the treatment of personal data. What happens if data privacy law encourages conduct that antitrust law or policy discourages, or even prohibits? When, and to what extent, should competition be traded at the margins for data

premise that the accumulation of certain data is capable of conferring monopoly power, which is the subject of scholarly disagreement. *See, e.g.*, Catherine Tucker, *Online Advertising and Antitrust: Network Effects, Switching Costs, and Data as an Essential Facility*, CPI ANTITRUST CHRON., Apr. 2019, at 3 ("Most studies suggest there are, at best, concave returns to data—that is, initially data can indeed provide performance advantages, but these performance advantages quickly decline as the firm obtains more data."); D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1136 (2016) (arguing minimal user data is required to gain a foothold in most online services).

50. Catherine Tucker, *Online Advertising and Antitrust: Network Effects, Switching Costs, and Data as an Essential Facility*, CPI ANTITRUST CHRON., Apr. 2019, at 6. The more specific the data collected about each consumer, the more targeted online advertising can be toward that consumer. This promotes robust advertising competition, because advertisers value that ad targeting and personalization. Privacy regulation may reduce the collection and use such data, which would reduce competition based on ad-targeting specificity.

51. *Consumer Data Rights and Competition Background: Note by the Secretariat*, ORG. FOR ECON. COOPERATION & DEV. ¶ 168 (June 12, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [https://perma.cc/YM84-8PJY].

52. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMMISSION iv (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/ZF4G-WBVL] (observing cautions from commentators about how privacy regulation could limit "the substantial consumer benefits made possible through the flow of information"); James C. Cooper & Joshua Wright, *The Missing Role of Economics in FTC Privacy Policy*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 465, 465 (Jules Polonetsky, Evan Selinger & Omer Tene eds., 2017) (observing that "[a]t its root, privacy regulation is about restricting information flows, which . . . are the lifeblood of today's digital economy").

privacy—or vice versa? The preoccupation with complementarity in existing theories has left enforcers, courts and companies with little insight on how to address these questions.

This is not to say that complementarity is an inaccurate description of the antitrust/data privacy interface—only that it is incomplete. As described above on the prevailing views, the interests of both areas of law can certainly be complementary. Nor does this Essay contend that every new antitrust case will pit data competition against data privacy, or even that most cases will. Information at issue in a given case may well be non-personal and unprotected by data privacy law. Or, competition may be driven by factors other than data in a particular market.

However, it is precisely the cases of tension, not complementarity, that will present agencies and courts with the most complex analytical challenges. Those cases will demand new analysis of tradeoffs between antitrust law and data privacy law. Further, those cases are likely to involve the complex businesses of digital platforms, which operate at the new nexus of antitrust and data privacy law. Despite this layered complexity, non-complementary interactions of privacy and antitrust have seen scant attention.

III. UNDERSTANDING TENSIONS AT THE NEW ANTITRUST/DATA PRIVACY LAW INTERFACE

This Part completes the picture of the new antitrust/data privacy law interface, by providing a descriptive, historical and comparative account of the tension between these areas of law. It begins with specific examples where competition and data privacy are increasingly at odds in the digital economy: business justifications and data access remedies. Then, it adds broader legal context, with the history of the antitrust/consumer protection law interface, and a comparative account of this intersection of law in the European Union. Both suggest tension on the horizon between antitrust and data privacy. This Part concludes with the early-stage observation that, when presented with tradeoffs between data privacy and competition, the existing theories, institutional mandates and early law indicate a likely bias toward competition over privacy.

A. Examples of Non-Complementarity Emerging in the Digital Economy

There are at least two specific areas of tension emerging between data privacy and antitrust law in the digital economy. First, digital platforms are invoking data privacy as a business justification to defend against allegations of anti-competitive conduct. Second, scholars and agencies are calling for remedies that grant access to the data held by digital platforms. Such remedies implicate data

privacy interests when they compel disclosure of consumers' personal data. Neither of these scenarios is addressed by existing theories. They fall within the lacuna of antitrust and data privacy law interaction as separate doctrinal areas of law, in a manner that is non-complementary.

1. *Data Privacy as a Business Justification for Alleged Anti-Competitive Conduct*

Dominant firms are invoking data privacy as a pro-competitive business justification for alleged exclusionary conduct. For Sherman Act sections 1 and 2 misconduct subject to a rule of reason standard,[53] the defendant may escape liability by proving it had a valid business justification for the alleged anticompetitive conduct.[54] The plaintiff must first establish a prima facie case that the defendant engaged in anti-competitive conduct. If this is shown, then the defendant is afforded the opportunity to prove that it had a pro-competitive business justification for its conduct. Where the defendant establishes such a business justification, the court will typically find there is no antitrust law violation.[55] In the past, intellectual property rights and consumer protection interests have both been invoked as business justifications—now the same is occurring for data privacy interests.

For example, the Ninth Circuit case *HiQ v. LinkedIn* described in the introduction to this Essay pitted HiQ's claims of anti-competitive exclusion against LinkedIn's justification of user data privacy protection.[56] The plaintiff, HiQ,

---

53. The rule of reason standard requires that the plaintiff prove the defendant has market power and engaged in conduct with an anti-competitive effect. This is in contrast with the "per se" standard, under which anticompetitive effects are inferred once the defendant is shown to have engaged in the conduct.

54. *See, e.g.*, LePage's Inc. v. 3M, 324 F.3d 141, 152 (3d Cir. 2003) (en banc), *cert. denied*, 542 U.S. 953 (2004) ("[A] monopolist will be found to violate § 2 of the Sherman Act if it engages in exclusionary or predatory conduct *without a valid business justification*." (emphasis added)).

55. United States v. Microsoft Corp., 253 F.3d 34, 57-58 (D.C. Cir. 2001). Once a justification is shown, the burden then returns to the plaintiff to show the harms from the anti-competitive conduct outweigh the business justification (in which case a violation is established). However, in practice, cases are almost always resolved before this final weighing stage in the analysis.

56. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). HiQ claimed under California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq. among other causes of action. However, HiQ's argument is very similar to a section 2 Sherman Act refusal-to-deal claim. In fact, the District Court looks to section 2 of the Sherman Act for guidance on what constitutes an anti-competitive act in state law. 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). Although the Ninth Circuit did not reach the unfair competition claim (because the tortious interference with contract claim was

scraped data from individual consumers' LinkedIn social network profiles, which the company then used to power its "people analytics" software.[57] Although LinkedIn initially permitted this access to user data, it later blocked HiQ from LinkedIn servers.[58] HiQ claimed its business could not survive without access to this LinkedIn user data. It argued the block constituted unfair competition, in service of LinkedIn's own plans to introduce competing data analytics software.[59]

LinkedIn defended its termination of HiQ's by invoking user privacy interests in profile data on the LinkedIn social network.[60] HiQ, it argued, was violating user data privacy by disregarding user profile settings.[61] LinkedIn is commonly used for professional networking. Changes to user profile information may therefore indicate an impending job search and employee departure. In fact, that was the premise of HiQ's software—alerting employers as to which of their employees are at risk for leaving their job, based on changes to the employee's LinkedIn profile.[62] The problem, LinkedIn argued, is that users had purposefully engaged a privacy setting called "do not broadcast" in order to prevent such profile changes from being automatically broadcast to their professional social network, including their employers' email inbox.[63] Regardless of whether users had engaged the "do not broadcast" setting, HiQ was reporting those very same profile changes to employers.

Both the district and circuit courts considered whether LinkedIn users had expectations of privacy over their public LinkedIn profile data. Ultimately, the courts were skeptical of LinkedIn's claim of user privacy protection, finding little concrete evidence of the privacy harm LinkedIn claimed would occur to users from HiQ's continued access to their profile information.[64] The Ninth Circuit

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 business justification for the conduct in tort law.

57. *hiQ Labs*, 938 F.3d at 991.

58. *Id.* at 991-92.

59. *Id.* at 998.

60. *Id*. at 994.

61. *Id*.

62. *Id.* at 990.

63. An estimated fifty million LinkedIn users chose to engage the "do not broadcast" setting. Once the setting is activated, changes made by the user to their profile are no longer sent via automated e-mail from LinkedIn to the contacts in the user's LinkedIn social network. When the setting is not engaged, everyone in the users' network receives an automated alert highlighting the changes in the user's profile. *Id.* at 994.

64. *Id*. at 994 (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), *aff'd*, 938 F.3d 985 (9th Cir. 2019)

upheld a preliminary injunction that required LinkedIn to restore HiQ's access to consumer profile data.[65] The injunction makes no mention of consumer data privacy settings, or how they might be accommodated for in the terms of HiQ's access.

This judicial skepticism toward user data privacy interests in *hiQ v. LinkedIn* is at odds with the FTC's regular efforts to protect similar consumer interests in online privacy settings. The FTC has pursued both Google and Facebook,[66] among other companies, for gathering data in violation of user data privacy settings, or for misrepresenting users' ability to rely on such settings to control who sees their information. As part of the new common law of data privacy, the FTC expects that digital platforms will honor user privacy settings—settings much like those disregarded by HiQ. If LinkedIn itself had violated the "do not broadcast" setting in the same manner as HiQ, LinkedIn could easily have faced section 5 FTC Act enforcement for misleading consumers about their ability to control the dissemination of their profile information.[67] Yet HiQ, a third-party with whom users may have no relationship, was given a court order enabling it to overrule consumers' chosen privacy settings. This remedy prefers data-driven competition over data privacy, at least at this preliminary stage of relief, with little explanation as to why that is better for consumers.[68]

Other digital platforms are similarly invoking data privacy as a business justification in response to allegations of anti-competitive conduct. Google, Apple and Facebook each face separate, but thematically similar, litigation or investigations alleging the companies excluded competing applications from their online platforms in violation of antitrust law.[69] For both Apple and Google, the claim is that competing apps have been barred from their respective online app stores—or at least, that the digital giants have refused to allow competitors access on

("[T]he actual privacy interests of LinkedIn users in their public data are at best uncertain . . . .").

65. *HiQ,* 938 F.3d at 1005.

66. *See* sources cited *supra* note 12.

67. 15 U.S.C. § 45(a)(1) (2018).

68. Instead, the Court emphasized the interest of HiQ in continuing to operate its business. To be fair, this was largely because the analysis was in the context of the balance of hardships analysis applied for preliminary injunctions. *hiQ Labs*, 938 F.3d at 995.

69. Many of these complaints hinge on the dual role of these digital platforms, who both exercise control over the sites of digital competition while also competing on those sites through vertically integrated offerings. For example, Facebook controls access of competing third party apps to its social media service, but also competes with some of the same apps to attract user attention and content. Critics claim this duality provides the power and incentive to refuse or limit rivals' access to such sites of competition under the guise of data privacy protection. *See* HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 5, at 39 (describing the "gatekeeper" role of large digital platforms).

terms equivalent to those of their own vertically integrated app offerings.[70] For Facebook the allegation is that the company excluded competing apps from its titular social media service, and the rich supply of user data that such access provides.[71] Though it is not yet clear which, if any, of these allegations amount to violations of antitrust law,[72] they are far from throwaway competitor complaints—European competition authorities are investigating some of the allegations against Apple,[73] and a complainant against Google has already obtained a preliminary injunction that ensured its access to Google's app store.[74] Importantly here, these digital giants have responded to the allegations by invoking

70. Natalia Drozdiak, *Google Play Store Rival Files Antitrust Complaint to EU*, BLOOMBERG (July 12, 2018, 6:23 AM PDT), https://www.bloomberg.com/news/articles/2018-07-12/google-play-store-rival-files-antitrust-complaint-to-eu [https://perma.cc/P9LE-EEXR] (describing the complaint of Aptoide, a competing app distribution storefront with the Google Play app store, which claims Google blocked and removed Aptoide from users' phones among other conduct). The complaint itself is not publicly available as of writing. *See also* Tom Warren, *Apple Faces Another EU Antitrust Complaint As App Store Pressure Grows*, VERGE (June 16, 2020, 5:08 AM EDT), https://www.theverge.com/2020/6/16/21292625/apple-rakuten-kobo-app-store-antitrust-complaint-europe [https://perma.cc/B8WN-UFEA] (noting complaints against Apple made to European antitrust authorities by Rakuten, Spotify, and Tile).

71. HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 5, at 168 (describing Facebook's termination of third parties' access to its titular social networking service, allegedly based on whether those companies posed a competitive threat, but also "in the wake of" the Cambridge Analytica privacy scandal); Fifth Amended Complaint of Plaintiff, Six4Three, LCC, for Injunction and Damages at 2, Six4Three, LLC v. Facebook, Inc., No. CIV 533328, 2018 WL 11190673 (Cal. Super. Ct. Jan. 12, 2018) (accusing Facebook of "anti-competitive schemes" that enticed software developers to create apps for Facebook, only to later deny those apps access to competitively important data). In this litigation, the "Pikini" app alleges Facebook terminated its access to data of users' friends in an anti-competitive manner. The privacy perspective is particularly at odds with this claim, given the FTC pursued Facebook, as part of the Cambridge Analytica scandal, for violating the FTC Act by *permitting* access to such users' friends data. *See* Press Release, Fed. Trade Comm'n, FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer [https://perma.cc/YC2B-PMV6].

72. In particular, the plaintiffs would need to prove an impact not just on themselves as competitors, but also on competition overall. Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., 429 U.S. 477, 488 (1977). This impact on competition is not clear from the initial reports on many of these allegations.

73. European Commission Press Release IP/20/1073, Antitrust: Commission Opens Investigations into Apple's App Store Rules (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 [https://perma.cc/53SK-DFDC] (opening an antitrust investigation into whether Apple's rules for the distribution of third-party apps via its App Store violate EU competition law).

74. Press Release, Aptoide, EU National Court Rules Against Google in Anti-Trust Process (Oct. 19, 2018), https://www.dropbox.com/sh/9eqm8ivrpwstjcz/AAC3f_jn3FWLxbTLDxeSTE4

their need to protect user data privacy and security, as justification for the impugned conduct.[75]

The allegations made by Tile, an app company, against Apple exemplify the pattern of privacy/competition tension arising in these cases. Tile makes hardware and a related application that enables users to track important objects, such as wallets or house keys. In Tile's complaint to European competition authorities, and in the recent House Report on Competition in Digital Markets, the company alleges that Apple impaired the ability of the Tile app to compete by favoring Apple's own, rival tracking app called "Find My."[76] Apple forces the Tile app to use the default "off" setting for consumer location tracking on Apple's popular mobile devices. Apple's own Find My app, in contrast, is allowed to use a default "on" settings for user location tracking.[77] Since users tend to accept default settings on apps, this seemingly small difference makes it much easier for Apple's app to obtain user location data. Both the Tile and Apple apps require that location data to operate—and to compete. In response to Tile's allegations, Apple has invoked its role in protecting user privacy, and cast itself as safeguarding sensitive user location data from third-party apps like Tile.[78] Apple claims

Ba/Press%20Release [https://perma.cc/X4JX-4Z4Z]. Though issued by a Portuguese national court, this injunction ensured access to the Google app store across the E.U. for the complaining app.

75. Dave Kleidermacher, *Android Security 2017 Year in Review*, GOOGLE SECURITY BLOG (Mar. 15, 2018), https://security.googleblog.com/2018/03/android-security-2017-year-in-review.html [https://perma.cc/Y4MF-J29M] (describing Google's position that it removes apps to protect users from malicious or unsecure app downloads); Adam Satariano, *Apple Defends App Store Policies After Spotify's Antitrust Complaint*, N.Y. TIMES (Mar. 15, 2019), https://www.nytimes.com/2019/03/15/business/apple-spotify.html [https://perma.cc/BYQ3-82AV] (describing Apple invoking consumer interests in the "App Store [being] a safe, secure platform" in response to Spotify's allegations of anti-competitive conduct).

76. HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 5, at 55 (testimony of Tile General Counsel pointing out the default setting difference and that Apple's FindMy app comes pre-installed on iPhones, unlike Tile's app, which users must install themselves); Monica Chin, *Apple Comes Out Swinging Against Tile After EU Complaint*, VERGE (May 29, 2020, 1:55 PM EDT), https://www.theverge.com/2020/5/29/21274709/apple-tile-european-commission-eu-complaint-app-store-iphone-response [https://perma.cc/XUX5-P9ED] (describing Tile's European complaint). Tile also complained that Apple has ceased selling Tile products in its physical stores. *Id*.

77. *See* Chin, *supra* note 76.

78. HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, *supra* note 5, at 55 (quoting testimony from Tile General Counsel that "Apple has used the concept of privacy as a shield" for disparate treatment of competitors); *id*. at 357 (Apple testimony indicating that disparate treatment of the applications is driven by difference in data storage that impacts privacy and security); Javier Espinosa, *Apple Accused of Competition Abuse Over Tracking Apps,* FIN. TIMES (May 28, 2020), https://www.ft.com/content/a08627c5-61d6-4513-9e7e-acac6b1ba862 [https://perma.cc/9C4Z-XZRF] (Apple invoking data privacy protection in response to Tile allegations of anti-competitive conduct).

the disparate treatment is merited, because Apple stores its app data locally on mobile device while Tile does not, creating greater potential privacy and security risks for user data on the Tile app.[79]

The Apple/Tile dispute presents legitimate and difficult questions about the tradeoffs between competition and data privacy. The FTC has recognized the privacy sensitivity of consumer location data, much like the data Tile and Apple both collect.[80] The agency has also emphasized the privacy significance between opt-out and opt-in consent to the collection of location data.[81] At the same time, it is plausible that competition between location-based apps would suffer from a lack of access to that same data. The main question will be whether overall competition is affected by Apple's conduct, or if it only impacts Tile. Assuming that could be shown, but also that Apple is legitimately protecting user privacy, how will privacy be accounted for in the antitrust analysis (if at all)?

Antitrust analysis has not yet addressed whether user data privacy protection is cognizable as a business justification. Separatist theory, by assuming away any interaction between these areas of law, does not reach this question. Integrationist theory could be applied to assess whether the asserted protection of data privacy improves consumer welfare, and is thus a potentially valid business justification.[82] However, no court, agency, or scholar has yet broached this analysis. Regardless, it is evident that these emerging scenarios do not fit into the existing narrative of antitrust/data privacy complementarity. Instead, they pit claims of anti-competitive conduct against the asserted business justification of consumer data privacy protection.

---

79. *Id*. at 357.

80. *See* Complaint, United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. June 22, 2016) (section 5 FTC Act claim against a mobile application that tracked users' physical location without their consent).

81. *Cross-Device Tracking: An FTC Staff Report*, FED. TRADE COMMISSION 15 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [https://perma.cc/X5MT-NB7L] (noting that companies should refrain from collecting and sharing location information unless there is "affirmative express consent" from the consumer being tracked).

82. Polygram Holding, Inc., 2003 WL 21770765 (F.T.C., July 24, 2003), *aff'd*, Polygram Holding, Inc. v. F.T.C., 416 F.3d 29, 36 (D.C. Cir. 2005) ("Cognizable justifications ordinarily explain how specific restrictions enable the defendants to increase output or improve product quality, service, or innovation.").

2. *Antitrust Behavioral Remedies May Grant Access to Private Consumer Data*

Antitrust behavioral remedies are another area of emerging yet largely unaddressed tension between antitrust and data privacy law. Scholars and some agencies are calling for antitrust remedies that compel access to, or disclosure of, consumer information held by digital platforms as a means of restoring online competition.[83] For example, the head of the EU competition authority warns that "as data becomes increasingly important for competition, it may not be long before the Commission [the EU-level competition authority] has to tackle cases where giving access to data is the best way to restore competition."[84] Litigation against digital platforms, particularly monopolization claims, may well end in behavioral remedies that grant rivals compulsory access to the user data held by those platforms.

Although data access remedies have been granted in past merger and conduct cases against technology companies,[85] contemporary remedies are distinguishable in their potential privacy impacts. Antitrust cases of old granted access to corporate information, such as business plans or technical data, like application

---

83. Reports to antitrust authorities in the United Kingdom and the European Union have recommended forced data sharing by large online companies to promote effective competition in digital markets. U.K. Digital Competition Expert Panel, *supra* note 38, at 74 ¶ 2.81 (2019) ("[I]n some markets, the key to effective competition may be to grant potential competitors access to privately-held data".); *Panel 2: Remedies for Competition Problems in Data Markets, Hearing #6: Privacy, Big Data, and Competition, Hearings on Competition and Consumer Protection in the 21st Century*, FED. TRADE COMMISSION 73-131 (Nov. 7, 2018), https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18_1.pdf [https://perma.cc/5G73-7W66] (discussing compulsory data access remedies).

84. Margrethe Vestager, Comm'r of Competition, Eur. Comm'n, Defending Competition in a Digitised World, Address at the European Consumer and Competition Day (Apr. 4, 2019), https://wayback.archive-it.org/12090/20191129202059/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/defending-competition-digitised-world_en [https://perma.cc/Q8P5-6N5W].

85. *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34, 46 (D.C. Cir. 2001) (requiring disclosures of APIs and other corporate data); United States v. Int'l Bus. Machs. Corp., No. 72-344, 1956 U.S. Dist. LEXIS 3992, at *29-30 (S.D.N.Y. Jan. 25, 1956) (ordering IBM to disclose technical information to the rivals); Intel Corp., 150 F.T.C. 420, 455-84 (2010) (requiring disclosure of roadmaps for future designs of chip interfaces). Though not "technology" companies as such, see also the data access remedies granted in *United States v. National Ass'n of Realtors*, 2008 WL 5411637 (N.D. Ill. Nov. 18, 2008)(requiring equal access to home listings data for online and traditional realtors); Agreement Containing Consent Order at 1, *In re Nielsen Holdings*, C-4439, 2014 WL 869523 (Sept. 20, 2013) (merger settlement mandating data access).

programming interfaces.[86] The defendant company owned and controlled the competitively important information, and therefore the compelled disclosure had no implications for privacy—it merely restored competition (or at least was expected to do so).

This is in stark contrast to the competitively important data held by today's technology giants, much of which relates to individual consumers and their potentially private online activities. Our search histories, social media activity and other online behavior fuel the services of, and competition with, many digital platforms. At the same time, the FTC's frequent pursuit of digital platforms under its de facto privacy authority indicates consumer privacy interests in large swathes of the data these companies hold. If access to such data is necessary to restore competition with digital platforms, that access may well erode the privacy of consumers. Mandated access seems at odds with FTC efforts to ensure consumers can control the collection and use of their private online data. There is little agency, judicial, or scholarly discussion of whether an antitrust data access remedy might be conditioned on consumer consent to disclosure, or whether consumer privacy interests even extend to such remedial disclosure of data.[87]

Are consumers better served by a remedy that increases data-driven competition, or by the incremental data privacy that remedy wears away? Again, the assumption of complementarity between data privacy and antitrust does not hold for this remedies dilemma. Data privacy law seems to be pursuing interests at odds with antitrust law, and cannot be reduced to a factor within the antitrust analysis.

B. Historical and Comparative Legal Contexts Foretell Tension Between Data Privacy and Antitrust Law

This Section argues that the tension emerging between antitrust and data privacy is predictable when considered in the broader historical and international legal context. First, it argues that antitrust law has a history of tension at its interface with consumer protection law, and that portends similar interactions with data privacy law. Second, it examines the European treatment of tension at the equivalent intersection of competition and data protection law, and argues that it foretells similar interactions in U.S. law.

---

86. *See* sources cited *supra* note 85.

87. *But see* Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 2, 80-86 (2020) (discussing consumer privacy interests in the context of antitrust data access remedies; arguing that consumer consent is not a robust long-term solution to the tension between data access remedies and data privacy).

1. *The Antitrust/ Consumer Protection Law Interface Suggests Tension is Likely with Data Privacy Law*

Though under-acknowledged, the tradeoffs between data privacy and competition are predictable based on the history of interaction between consumer protection law and antitrust law. Since U.S. data privacy law arose from consumer protection law—both are based on enforcement of section 5 of the FTC Act— we can expect that similar interactions will occur where data privacy meets antitrust law.

Much like data privacy, consumer protection law is often cast as complementary with antitrust.[88] The goal of antitrust is to advance consumer welfare through competition.[89] This is often consistent with consumer protection law, which seeks to protect individual consumers from unfair and deceptive practices in the marketplace.[90] Generally, the protection of consumers ought to improve their welfare. Antitrust law and consumer protection law have been called "sisters under the skin," reflecting this macro-level similarity in their goals.[91]

Despite this, competition and consumer protection law can also clash at the margins.[92] When consumer protection efforts stray too far into the marketplace,

---

88. *See, e.g.*, Julie Brill, *Competition and Consumer Protection: Strange Bedfellows or Best Friends?*, ANTITRUST SOURCE (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/competition-and-consumer-protection-strange-bedfellows-or-best-friends/1012abamasternewsletter.pdf [https://perma.cc/SZU8-XHMD] (noting that consumer protection and antitrust law "share the common goal of addressing distortions in the marketplace"); Thomas B. Leary, Comm'r, Fed. Trade Comm'n, Remarks on Self-Regulation and the Interface Between Consumer Protection and Antitrust (Jan. 28, 2004), https://www.ftc.gov/sites/default/files/documents/public_statements/self-regulation-and-interface-between-consumer-protection-and-antitrust/040128deweyballantine.pdf [https://perma.cc/L927-734R] (observing that the goals of antitrust and consumer protection law are compatible).

89. Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979) ("Congress designed the Sherman Act as a 'consumer welfare prescription.'"). Although the desirability of the consumer welfare standard is debated, it remains the widely accepted goal of antitrust law. *See, e.g.*, Christine S. Wilson, Comm'r, Fed. Trade Comm'n, Welfare Standards Underlying Antitrust Enforcement: What You Measure Is What You Get, Keynote Address at the George Mason Law Review 22nd Annual Antitrust Symposium: Antitrust at the Crossroads? (Feb. 15, 2019), https://www.ftc.gov/system/files/documents/public_statements/1455663/welfare_standard_speech_-_cmr-wilson.pdf [https://perma.cc/GW25-TWNM] (noting that the consumer welfare standard has been "the yardstick used to evaluate mergers and competitive conduct for more than 40 years" in antitrust law).

90. *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc [https://perma.cc/K2PP-ADXY] (articulating the strategic goal of consumer protection).

91. Leary, *supra* note 88, at 1.

92. *See id.* at 2 (acknowledging consumer protection and antitrust can "clash at the margins" despite their similar objectives); *see also Leary: Consumer Protection-Antitrust Conflict*, *supra* note 47 (observing similar tension).

that can constrain rivals' ability to compete, and cause a corresponding reduction in consumer welfare.[93] On the other hand, competition entirely unbridled by consumer protection law leads to deceptive and unfair commercial conduct, which also harms consumers. Maximum consumer welfare lies somewhere between the extremes of each area of law. The result, as FTC Commissioner Julie Brill describes, is an overall legal intersection that is not just complementary but rather multi-modal: "Sometimes the principles at the heart of these two areas of law point to conflicting results, while at other times they work in harmony towards the same end."[94]

The FTC has brought several challenges to trade and professional association rules that exemplify this potential for the two areas of law to point to conflicting results. Under its competition mandate, the FTC has long advocated against professional association rules that restrain the association members' ability to advertise or to engage in other pro-competitive conduct. The agency has challenged the rules of associations of funeral directors,[95] lawyers,[96] doctors,[97] chiropractors,[98] dentists[99] and optometrists[100] as conspiracies in restraint of trade or other violations of section 5 of the FTC Act.

In some cases, the challenged rule is an obvious cover for industry collusion, and "no elaborate industry analysis is required to demonstrate the anticompetitive character of [the] agreement."[101] In these cases, there is no genuine tension

---

93. Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy: The Interface of Competition and Consumer Protection (Oct. 31, 2002).

94. Brill, *supra* note 88, at 1.

95. *See, e.g.*, Va. Bd. of Funeral Directors and Embalmers, 138 F.T.C. 645 (2004) (describing a restriction of competition by prohibiting advertisement of discounts for advance funeral planning and services).

96. *See, e.g.*, Fed. Trade Comm'n & Dept. of Justice, Comment Letter on Proposed Definition of the Practice of Law Before the Supreme Court of Hawaii (Apr. 20, 2009), http://www.ftc.gov/os/2009/04/V080004hiunauthorizedpracticeoflaw.pdf [https://perma.cc/2PNM-BLBM] (restricting nonlawyers from competing with lawyers).

97. *See, e.g.*, Am. Med. Ass'n, 94 F.T.C. 701 (1979), *aff'd sub nom.* Am. Med. Ass'n v. FTC, 455 U.S. 676 (1982) (finding that AMA ethical guidelines suppressed truthful advertising).

98. *See, e.g.*, *In re* Conn. Chiropractors Ass'n, 114 F.T.C. 708 (1991) (consent order) (opposing restriction on truthful advertising of free services, considered "undignified" by the association).

99. FTC v. Ind. Fed'n of Dentists, 476 U.S. 447 (1986).

100. *See, e.g.*, *In re* American Acad. of Optometry, Inc., 108 F.T.C. 25 (1986) (rejecting the restriction on all truthful advertising and solicitation).

101. *Ind. Fed'n of Dentists*, 476 U.S. at 459 (quoting Nat'l Soc. of Prof'l Eng'rs v. United States, 435 U.S. 679, 692 (1978), and holding that no elaborate analysis was required to conclude a policy of withholding x-rays from insurers is anti-competitive).

between competition and consumer protection, because there is no genuine consumer protection interests at stake.

However, other cases, like *California Dental Association v. FTC*,[102] raise a difficult and legitimate conflict between competition and consumer protection interests. The defendant dental association enacted rules that limited member dentists from advertising about price discounts and service quality unless the dentists included extensive disclosures.[103] Applying an abbreviated rule-of-reason ("quick look") analysis, the Ninth Circuit affirmed the FTC's conclusion that the association rules violated section 5 of the FTC Act.[104] The onerous rules unreasonably restricted truthful advertising, which reduced ad-based price and quality competition for dental services, to the detriment of consumers.[105]

The Supreme Court reversed. The Ninth Circuit had too quickly dismissed the dental association's justification of consumer protection.[106] The dental association argued its advertising rules were important to prevent members from engaging in false or misleading advertising about pricing or quality, which protected consumers from unsubstantiated dental advertising claims.[107] The Supreme Court concluded that the dental services market was characterized by "striking" information asymmetries between dentists and patients, which made it challenging for patients to make informed decisions.[108] It was plausible that in such a market, the association's advertising rules did, in fact, protect consumers, by making it easier for patients to comparison shop and by preventing dentists from making misleading advertising claims.[109] The Supreme Court even speculated that the consumer protection benefits of the association rules might outweigh their costs to competition, though this determination was left to the lower court on remand.[110] The Supreme Court vacated and remanded for further consideration under a more searching rule-of-reason standard.[111]

---

102. 526 U.S. 756 (1999).

103. *In re* Cal. Dental Ass'n, 121 F.T.C. 190, 192 (1996), *aff'd sub nom.* Cal. Dental Ass'n v. FTC, 128 F.3d 720 (9th Cir. 1997), *vacated*, 526 U.S. 756 (1999).

104. Cal. Dental Ass'n v. FTC, 128 F.3d 720, 726-30 (9th Cir. 1997), *vacated*, 526 U.S. 756 (1999) (finding a violation of section 1 of the Sherman Act, 15 U.S.C. § 1 (2018), and consequently section 5 of the FTC Act, 15 U.S.C. § 45 (2018)).

105. *Cal. Dental Ass'n*, 128 F.3d at 727.

106. *Cal. Dental Ass'n*, 526 U.S. at 772-73.

107. *Id*. at 763, (describing the dental association's pro-competitive justification argument).

108. *Id*. at 771.

109. *Id*. at 771-74.

110. *Id*. at 775.

111. *Id*. at 781.

On remand, the Ninth Circuit found that the dental association had strong evidence of consumer protection effects from the advertising restrictions.[112] Consistent with the Supreme Court's suggestion, the Circuit also found that the pro-competitive benefits of consumer protection from the association's rules outweighed the FTC's limited evidence of anti-competitive effects.[113]

This saga of association advertising rules illustrates the tension at the margins between consumer protection and competition-driven consumer welfare. Though often explained as complementary, competition and consumer protection interests were at odds in this case.

A similar tension has appeared more recently, in the FTC's opposition to state and municipal regulation of online funereal supply[114] and online ride-sharing.[115] States and municipalities have passed new regulations for these online industries with the intent of protecting consumer health and safety.[116] The FTC is concerned that the new regulations will limit these online entrants from competing with industry incumbents,[117] such as taxis (for online ride-sharing), and traditional brick and mortar funeral homes (for online funeral supply). The FTC has opposed certain new regulations through litigation[118] and counseled regulatory

---

112. Cal. Dental Ass'n v. FTC, 224 F.3d 942, 957 (9th Cir. 2000).

113. *Id.* at 958 (concluding that no "net anticompetitive effect" arises from the dental association's rules). On further remand back to the FTC, the FTC dismissed the case, but with a statement emphasizing that the agency would continue to challenge anti-competitive association advertising rules. *In re* Cal. Dental Ass'n, No. 9259, 2001 WL 34686091, at *2 (F.T.C. 2001).

114. *See, e.g.*, Memorandum of Law of Amicus Curiae the FTC at 1, Powers v. Harris, No. CIV-01-445-F, 2002 WL 32026155 (W.D. Okla. 2002) [hereinafter FTC Challenge to Online Funeral Supply Regulation] (challenging as anti-competitive a state law that restricted online sales of caskets to licensed funeral directors that purported to protect consumers).

115. Directorate for Fin. & Enter. Affairs Competition Comm., *Taxi, Ride-sourcing and Ride-sharing Services—Note by the United States*, ORG. FOR ECON. COOPERATION & DEV. 4-6 (June 4, 2018), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/taxi_united_states.pdf [https://perma.cc/3DYJ-H9GN] (summarizing FTC staff comments on ride sharing regulation). Ride-sharing services, such as Uber and Lyft, act as digital platforms that connect individual drivers to consumers seeking a ride.

116. Regulation of ride-sharing services in the interest of consumer safety has included, for example, requirements that accidents be reported, that vehicles meet certain safety standards, and that drivers be subject to background-checks.

117. *See, e.g.*, *Staff Comment to the Hon. Brendan Reilly Concerning Chicago Proposed Ordinance O2014-1367 Regarding Transportation Network Providers*, FED. TRADE COMMISSION 1 (Apr. 15, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-honorable-brendan-reilly-concerning-chicago-proposed-ordinance-02014-1367/140421chicagoridesharing.pdf [https://perma.cc/8BBX-EXCH] (expressing concern that certain provisions of ride sharing regulations will "unnecessarily impede competition from these services").

118. *See* FTC Challenge to Online Funeral Supply Regulation, *supra* note 114.

restraint through agency advocacy.[119] As in *California Dental*, consumer protection and competition are at odds at the margins in these matters. The FTC draws the appropriate tradeoff between the two interests at a different point than certain state and municipal actors.

This history of tradeoffs at the edges of consumer protection and competition suggests similar interactions will arise between data privacy and antitrust law. Data privacy law is a subcategory of consumer protection law in the United States. Such closely related areas of law are likely to have similar modes of interaction with antitrust. Like the intersection with consumer protection, we might expect that competition and data privacy are complementary in many cases—which perhaps explains why theories have focused on such complementarity so far. But we should also expect to see certain cases in which data privacy and antitrust interests are at odds at the margins.

Such tension is already emerging in the digital economy when privacy is asserted as a business justification for anti-competitive conduct, and in calls for remedies that grant access to data on digital platforms.[120] Further, it is easy to imagine a scenario akin to that of *California Dental*, where data privacy, rather than consumer protection, is invoked in defense of allegedly collusive conduct. An association might, for example, adopt a new privacy-enhancing rule that prohibits its members from using consumer data for targeted online advertising. Like the challenged rules in *California Dental*, such a restriction could also be cast as reducing ad-based price competition.

Where data privacy and competition are not complementary, the consumer welfare tradeoffs are likely to be complex. The winding history of cases like *California Dental* and the recent FTC action on online industry regulation, suggest that various courts, agencies, and branches of government may also differ on where to draw the appropriate balance between the interests of competition and data privacy.[121] Given this impending complexity, it is time to consider how to navigate tension at the new antitrust/data privacy interface.

---

119. *See* Directorate for Fin. & Enter. Affairs Competition Comm., *supra* note 115 (summarizing FTC ride-sharing advocacy).

120. *See supra* Section III.A.

121. For example, in *California Dental*, the FTC and lower courts diverged from the Supreme Court on their view of the appropriate tradeoff between consumer protective rules and competition. The Ninth Circuit, with additional insight from the Supreme Court, drew the balance in a different position on remand than in its initial decision. Similarly, state and municipal regulators differ from the FTC in their views of where the appropriate balance lies for ride sharing and other online industry regulation.

2. *The European Competition Law/Data Protection Interface Indicates Tension on the U.S. Horizon*

The European Union experience at the intersection of data privacy and antitrust law foretells tension between these two areas of law in the United States.

The obligations and the enforcement of European data protection law and competition law tend to be more robust than their U.S equivalents. Data privacy is a fundamental right in the European Union, protected by constitutional law and, as of May 2018, the wide-reaching new privacy regulation, GDPR.[122] This rights conception often translates into stronger data privacy protections than those afforded by U.S. law, where the jurisprudential roots are only as deep as consumer protection doctrine. For example, the European Union prohibits processing of personal information by default; protected data may only be collected, transferred, and used when permitted by law. American privacy law takes the opposite baseline position—data use is de facto permitted, unless the law states otherwise.[123]

European competition law, particularly the prohibition on abuse of dominance, is also more onerous than its Sherman Act equivalent.[124] For example, European competition law imposes special obligations on dominant firms, which makes it easier to bring unilateral conduct cases under E.U. law.[125] There is no equivalent U.S. legal obligation on monopolist firms. European competition authorities have also been significantly more active than their U.S. counterparts in pursuing abuse of dominance cases against large technology platforms. The European Commission has several ongoing investigations into technology

---

122. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, 397 art. 8 (describing a fundamental right to "the protection of personal data"); GDPR, *supra* note 3, (protecting the privacy of "natural persons with regard to the processing of personal data and the free movement of such data").

123. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880-81 (2014) (observing this distinction in the default data privacy law positions of the United States and the European Union).

124. Consolidated Version of the Treaty on the Functioning of the European Union, May 9, 2008, 2008 O.J. (C 115), Art. 102. This European prohibitions on abuse of dominance are roughly equivalent to the U.S. monopolization prohibitions found in section 2 of the Sherman Act. 15 U.S.C. § 2 (2018).

125. *See, e.g.*, Case T-321/05 AstraZeneca AB and AstraZeneca plc v. Comm'n, 2010 E.C.R. II-02805, at ¶ 355 (discussing the "special responsibility" of dominant undertakings under European competition law).

giants,[126] and has already imposed multiple fines on Google for abuse of dominance.[127]

In the face of more robust antitrust and data protection laws, European competition agencies and scholars have already begun to examine the interaction of these two areas of law in earnest.[128] There is a new but growing body of literature and agency reporting that maps the varying modalities of interaction between competition and data protection law, including potential conflicts. The scholarship recognizes that data protection and competition law can be either complementary or in tension,[129] considers whether GDPR would prohibit data processing for the purposes of an antitrust data access remedy, [130] and considers whether data privacy may constitute a business justification for anti-competitive conduct.[131] There is little consensus on these emerging issues, but this European work acknowledges and begins to theorize the tension between antitrust and data privacy law in a manner absent from the U.S. dialogue.

Some might explain away this European experience as inapplicable to U.S. law and policy. As canvassed above, there are legitimate distinctions to be drawn between U.S. and E.U. law. In particular, the existence of data privacy as a right in European Union law may strengthen the rationale for considering privacy in

126. *See* sources cited *supra* note 6 (investigations by European competition authorities into Apple and Amazon for alleged abuse of dominance).

127. *See id.* (noting that European competition authorities have fined Google three times recent years for abuse of monopoly).

128. *See, e.g.*, Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer, *Competition Policy for the Digital Era*, EUR. COMMISSION 73 (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf [https://perma.cc/PH74-UD9B] (discussing "interdependency between competition law and data protection law"); Vestager, *supra* note 34 (noting that competition policy "will have to give companies access to the data they need to compete . . . and it will have to respect the privacy rights of the people whose data it is"); *infra* sources cited notes 129-131.

129. *See* Inge Graef, Thomas Tombal & Alexandre de Streel, *Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law* 20-26 (Tilburg Law & Econ. Ctr., Discussion Paper No. 2019-024, 2019).

130. Crémer et al., *supra* note 128, at 98-108; INGE GRAEF, EU COMPETITION LAW, DATA PROTECTION AND ONLINE PLATFORMS: DATA AS ESSENTIAL FACILITY 312 (2016) (arguing that the GDPR exception permitting processing pursuant to a "legal obligation" would be a legitimate basis for data processing pursuant to a remedy); Vikas Kathuria & Jure Globocnik, *Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy*, J. ANTITRUST ENFORCEMENT (Jan. 19, 2020), https://doi.org/10.1093/jaenfo/jnz036 [https://perma.cc/H6NS-93HY] (arguing against mandatory data access as an antitrust remedy in data-driven markets, and that the GDPR would not permit such processing).

131. *See* Torsten Körber, *Is Knowledge (Market) Power? – On the Relationship Between Data Protection, 'Data Power,' and Competition Law* 30 (Jan. 29, 2018), https://ssrn.com/abstract=3112232 [https://perma.cc/TTB4-5DR5] (arguing that data protection should not be recognized as a business justification in European competition law).

antitrust analysis.[132] These differences may lead some to conclude that tension is not under-acknowledged in the United States, as this Essay argues, but rather nonexistent.

However, it would be a mistake to assume these differences render the European experience irrelevant. Both U.S. data privacy law and anti-monopolization law are undergoing eras of expansion. These developments nudge the American legal landscape closer to that of the European Union, and renders the E.U.'s equivalent interactions of law increasingly instructive, even if not identical to the United States.

The expansion of U.S. data privacy law is apparent by many different measures. There have been numerous proposals to enact omnibus federal data privacy protection legislation,[133] and the concept has raised bipartisan support. In the interim, the FTC is expanding the new common law of data privacy, moving beyond the agency's early enforcement of company privacy promises to require more robust, baseline privacy protections rooted in consumers' reasonable expectations of privacy.[134] The scope of data considered "personal," and thus subject to such reasonable expectations, is ever-expanding, as we better understand the potential for cross-identification and de-anonymization in digital environments.[135] State data privacy law is also expanding, with the first ever broad-

132. *See, e.g.*, Peter Swire, Professor of Law, Ohio State Univ., Ctr. for Am. Progress, Presentation on Privacy and Antitrust at the IAPP Spring Conference 10 (Mar. 2008), https://peterswire.net/speeches [https://perma.cc/RJ3Y-NDQS] ("In Europe, privacy [is] clearly a fundamental right. . . . That strengthens the case for privacy concerns to be explicitly considered in E.U. competition review.").

133. *See, e.g.*, Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020) (providing privacy protection for 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) (same); 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).

134. Solove & Hartzog, *supra* note 13, at 661-62 (observing this expansion in FTC enforcement).

135. *See* President's Council of Advisors on Sci. & Tech., *Big Data and Privacy: A Technological Perspective*, EXECUTIVE OFF. PRESIDENT 38 (May 2014), https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/2U2T-LYCZ] ("[I] . . . t is increasingly easy to defeat anonymization by the very techniques that are being developed for many legitimate applications of big data.").

based data privacy protection statute enacted in California in 2018,[136] and other states passing recent biometric and facial-recognition data protection laws.[137]

At the same time, there is renewed agency and political will to enforce U.S. antitrust laws.[138] Some scholars label this rise of both U.S. data privacy regulation and antitrust law the "Brussels Effect," referring to the exportation of EU legal standards through their influence on foreign nations.[139] The European experience at this interface of law is thus relevant to the U.S. The European perspective indicates that, as antitrust and data privacy become "bigger" in the U.S., the interaction between these areas of law will become more expansive and complex as well. The European literature also confirms that not all of these newfound interactions will be complementary, as U.S. theories have so far tended to presume.

If privacy becomes a personal and fundamental right in the United States, as some argue it should be,[140] that would even raise the potential for a European-style hard conflict between the obligations imposed by data privacy law and those under antitrust law. Certainly the "rights talk" conception of European privacy law has been spilling over into U.S. political discourse and state legislation.[141] But, even if data privacy remains a consumer protection interest in U.S. law, the current expansion of that interest will present growing tradeoffs with data-driven competition. Though the magnitude of the collision may be less than in the European Union, we can expect to see similarly expanding tension at the interface of U.S. antitrust law and data privacy.

---

136. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2020).

137. *See, e.g.*, DEL. CODE ANN. tit. 6 §§ 1201C-1206C (West 2020) (asserting that mobile applications must comply with certain privacy protection measures, such as displaying a privacy policy); 740 ILL. COMP. STAT. ANN. 14/15 (West 2019) (establishing privacy protection of biometric information); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019) (same).

138. *See supra* notes 4-5 and accompanying text (describing the recent revival of U.S. antitrust law and policy focused on digital platforms).

139. 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).

140. *See, e.g.*, Complaint and Request for Injunction, Request for Investigation and for Other Relief at 2, *In re* Google, Inc. (Apr. 20, 2007) (FTC File No. 071-0170), https://epic.org/privacy/ftc/google/epic_complaint.pdf [https://perma.cc/G9E9-SC3N] (arguing that the right of privacy is a personal and fundamental right).

141. *See, e.g.*, CAL. CIV. CODE § 1798.100 (West 2020); 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/8C84-7HFX] (proposing a "Consumer Privacy Bill of Rights"). The Consumer Privacy Bill of Rights is rooted in the FIPPS, which were themselves framed in relation to the "rights of citizens." DEP'T OF HEALTH, EDUC. & WELFARE REPORT, *supra* note 13, at 50 (articulating the FIPPS).

C. Competition is Likely to be Preferred over Data Privacy

The necessary implication of tension at the new antitrust/data privacy interface is that choices will have to be made between competition and privacy interests. This Section suggests that competition is likely to be preferred over privacy and observes very early indications this may already be occurring—whether or not that preference is justified, or even acknowledged.

Existing theories and institutional context create a "competition first" perspective at the intersection of antitrust and data privacy. The leading theory—the integrationist view—treats data privacy as a factor to be subsumed into existing antitrust understanding.[142] This makes sense, given that the origin of the theory is, of course, antitrust law. However, this also builds into the analysis a perspective of competition primacy. The institutions involved reinforce this primacy. It is predominantly agencies of antitrust,[143] not of data privacy, that are considering the implications of this intersection of law. The mandate of antitrust agencies is to advance competition, not privacy. In fact, antitrust agencies have expressed skepticism as to whether they have jurisdiction over interests of data privacy.[144] In this theory and agency context, the tendency will thus be to prefer competition when faced with a data privacy tradeoff.

Competition primacy is predictable from the courts as well, because data privacy harms remain emergent and often ill-defined in law.[145] The FTC has faced resistance from courts on jurisdictional grounds when it alleges only soft, nonfinancial privacy harms, such as risk of identity theft, in its complaints.[146] Amorphous privacy harms can be difficult to substantiate with adequate evidence, and so tend to be afforded minimal weight in balancing against more readily articulated and evidenced harms—like those to competition. Daniel J. Solove observes a similar phenomenon where data privacy is being balanced against other (non-

---

142. *See supra* Part I.

143. Or Bureaus, in the FTC's case.

144. Statement of FTC Concerning Google/DoubleClick, *supra* note 30, at 2 (finding a lack of jurisdiction to intervene in the transaction based on asserted privacy harm).

145. 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.")

146. *See, e.g.*, Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, 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 re* LabMD, Inc., No. 9357, 2015 WL 7575033, at *41-43 (F.T.C. Nov. 13, 2015), *rev'd*, 2016-2 Trade Cas. (CCH) 79708 (2016), *aff'd on other grounds*, LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018) (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, reputational or other similar harms).

antitrust) interests like free speech or data security, which are more readily articulated and weighed against ill-defined data privacy interests.[147]

Though in its early stages, this hypothesis of bias seems to be emerging in cases like *HiQ v. LinkedIn*. The Ninth Circuit found LinkedIn presented "little evidence" of the claimed consumer privacy interests in social media profile data and settings.[148] Even if users have privacy interests in their LinkedIn data, the court found that those interests were not significant enough to outweigh HiQ's interest in continuing its business, at least at the preliminary injunction stage.[149]

All of this may mean countervailing data privacy interests are prone to being too easily discounted, much like the consumer protection interests were in the saga of *California Dental*. Particularly at this early stage of understanding the antitrust/data privacy law interface, we should resist an automatic preference for competition. Any such preference would rely on unexamined assumptions that competition is always preferable to privacy in its effects on consumer welfare, which seems like a premature conclusion. Instead, where competition is preferred, that preference ought to be considered and justified with an analysis that accounts for both interests. Acknowledging the tradeoffs between data privacy and competition that are emphasized in this Essay is a necessary first step to develop such an analysis.

IV. A PROPOSAL FOR ANALYSIS AT THE NEW ANTITRUST/DATA PRIVACY LAW INTERFACE

This Part proposes an initial approach to analyze claims of tension at the new antitrust/data privacy law interface. This proposal begins to fill in the gaps left by existing theories by considering how antitrust law and data privacy law interact as separate, non-complementary doctrinal areas of law.

When a legitimate but countervailing privacy interest is raised in an antitrust dispute,[150] the analytical starting point should be to grant equal billing to both areas of law. This means that in determining the scope of permitted conduct, neither antitrust law nor privacy law would be presumed to have primacy over the other. Nor would conduct that is encouraged or required by one area of law

147. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 7-8 (2008).

148. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 994 (9th Cir. 2019).

149. *Id.* at 995.

150. As with the antitrust/consumer protection interface, there may also be easy cases where the asserted data privacy interests are merely being invoked as cover for anti-competitive acts. In such cases, there is no real tradeoff at stake. By analogy to consumer protection cases, "no elaborate industry analysis is required" for courts or agencies to reject the claimed privacy interest. FTC v. Ind. Fed'n of Dentists, 476 U.S. 447, 459 (1986) (quoting Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 692 (1978)).

be considered necessarily immune from the other area of law. Instead, the importance of the respective interests at stake in antitrust and data privacy should be considered and then weighed against each other.

In practice, application of this approach will require courts and agencies to delve into the strength of the specific data privacy and competition interests at stake. This would include considering, on one hand, the centrality or importance of the principle being invoked in data privacy law, and, on the other hand, the degree to which competition is impeded by the alleged misconduct. Traditional antitrust assessments of anti-competitive effects and market power would remain relevant, but potentially offsetting legal considerations related to data privacy would also be considered. Those offsetting considerations would be determined with reference to data privacy law, and the reasonable expectations of privacy recognized in it. This analysis could look much like the rule-of-reason analysis in *California Dental*, where the court considered how the specific market context informed the strength of the claimed consumer protection interests. The difference is that the analysis here would be specific to data privacy harms, rather than general consumer protection considerations.

This proposed analytical paradigm is modeled on approaches that have developed over time at the intersections of antitrust with other major doctrinal areas of law, like patent and consumer protection. For example, over their shared history, patent and antitrust law have long vacillated between primacy of one area of law or the other, as reflected in various judicial presumptions and agency guidance.[151] However, as theories of this intersection developed over time, many of these simplifying presumptions were dropped.[152] In their place, the most recent Supreme Court case on the antitrust/patent interface emphasizes that both

---

151. *See, e.g.*, Int'l Salt Co. v. United States, 332 U.S. 392 (1947) (recognizing a presumption that a patent conferred market power, which made it easier to establish violations of antitrust law by patent holders), *overruled by* Illinois Tool Works Inc. v. Independent Ink, Inc., 547 U.S. 28 (2006); FTC v. Watson Pharm., Inc., 677 F.3d 1298, 1312 (2012) (categorizing conduct within the "scope of patent" rights as immune to antitrust scrutiny of reverse payment settlements in patent infringement litigation), *rev'd sub nom.* FTC v. Actavis, 570 U.S. 136 (2013); Bruce B. Wilson, Deputy Assistant Attorney Gen., Antitrust Div., Remarks Before the Annual Joint Meeting of the Michigan State Bar Antitrust Law Section and the Patent Trademark and Copyright Law Section: Is the Past Prologue, or Where Do We Go From Here?, *in* 5 TRADE REG. REP. ¶ 50,146 (Sept. 21, 1972) (describing the licensing practices that became known as the "Nine No-No's," which prohibited intellectual property licensing practices presumed to harm competition).

152. Illinois Tool Works Inc. v. Independent Ink, Inc., 547 U.S. 28, 31 (2006) (overturning the *Int'l Salt Co.* presumption that a patent confers market power). The equivalent presumption had already been eliminated in patent law through 1988 amendments to the Patent Act. Pub. L. No. 100-703, 102 Stat. 4674 (1988) (codified at 35 U.S.C. § 271(d) (2018)); *see also* FTC v. Actavis, 570 U.S. 136, 149 (2013) (rejecting the "scope of patent" approach that had immunized many reverse payment settlements from antitrust scrutiny); Richard Gilbert & Carl

patent and antitrust policies are relevant to determining the scope of conduct permitted by a patent rights holder.[153] The decision expressly rejects a lower court approach that assumed primacy of patent law and instead encourages courts to seek an "accommodation" that strikes a balance between patent and antitrust.[154]

Under this approach, the interests of both areas of law are recognized, and shape their intersection. If antitrust law oversteps and impedes efficient, legitimate uses of patent rights, it can undermine patent law-created incentives for innovation. Conversely, if patents are upheld despite being invalid or overbroad in their enforcement, those patent "rights" disrupt competition, by discouraging follow-on innovation with unmerited licensing costs and litigation.[155]

Cases like *California Dental* reflect a similar approach of accommodation at the antitrust/consumer protection interface, though it is not described this way in the decision. When consumer protection is invoked without justification, or strays too far, it impedes the value-driving effects of competition and harms consumer welfare.[156] When competition is unbridled by the limits on deception and unfairness imposed by consumer protection law, that competition reduces, rather than improves, consumer welfare. These areas of law and policy are mutually defining, with each reining in the other.

The approach proposed here affords similar, mutual relevance to each area of law in shaping the antitrust/data privacy interface. It recognizes that if data privacy interests are over-expanded or interpreted beyond their appropriate scope, that interferes with legitimate and beneficial uses of data to compete. Such an interpretation of data privacy would undermine the benefits to consumers from the use of their data, such as free and personalized digital services. Conversely, if antitrust law or competition policy oversteps, going too far in their

Shapiro, *Antitrust Issues in the Licensing of Intellectual Property: The Nine No-No's Meet the Nineties* 286, BROOKINGS INSTITUTION (1997), https://www.brookings.edu/wp-content/uploads/1997/01/1997_bpeamicro_gilbert.pdf [https://perma.cc/ZG8T-ZP57] (describing the abandonment of the categorical prohibitions in the Nine No No's, in favor of rule-of-reason analysis for the licensing practices that recognized their potentially pro-competitive nature).

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

154. *Id*. at 136.

155. FED. TRADE COMM'N, THE EVOLVING IP MARKETPLACE: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION 1 (March 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/M23J-7NV3].

156. Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy: The Interface of Competition and Consumer Protection (Oct. 31, 2002) ("Without a continuing reminder of the benefits of competition, a consumer protection program might tend to impose controls that ultimately may diminish the very competition that increases consumer choice.").

compromise of legitimate data privacy protections in the name of competition, that also harms consumers.

This accommodative approach makes sense for the new antitrust/data privacy interface. It draws on the wisdom of more extensively theorized intersections between antitrust and other areas of law. At the same time, it corrects for an otherwise-likely bias of theories, agencies and courts toward a preference of competition over data privacy.[157] Instead of allowing this unexamined competition primacy, the proposed approach reorients to a starting position that grants equal billing to both areas of law. It automatically prefers neither. As courts and agencies become more familiar with the antitrust/data privacy law interface, their repeated analysis of similar conduct may enable presumptions or shorter-form analysis of related consumer welfare tradeoffs. Until then, this Essay calls for an approach that considers the strength of the interests at stake in both areas of law.

CONCLUSION

We are only beginning to understand the interactions between data privacy, competition, and related law. So far, antitrust theories have either cast data privacy as a quality-like factor within antitrust analysis, or dismissed privacy as an entirely separate legal issue. Under both views, data privacy interests tend to be explained away as complementary with those of competition.

Such characterizations may often be accurate, but this Essay argues they are also incomplete. Particularly for digital services, antitrust and data privacy law share a multi-modal interface, at times complementary, and at times in tension. By focusing only on complementarity, existing theories leave unexamined the more complex situations where data privacy is traded at the margins for data-driven competition, or vice versa. In particular, theories tend to overlook the role of data privacy law as a distinct area of legal doctrine that, at times, pursues interest at odds with those of antitrust law.

This Essay adds a new facet to our understanding of the antitrust/data privacy interface, with a descriptive, historical and comparative account of tension between the two areas of law. It presents the related history between antitrust and consumer protection law, and describes the comparative European legal perspective. Both indicate an impending clash on the horizon between these two areas of law. This reality of tension is already materializing in claims that data privacy is a business justification for anti-competitive conduct and in calls for antitrust remedies that grant access to potentially private consumer data.

---

157. *See supra* Part III.C.

This Essay concludes with a proposed approach to analyzing tension at the new antitrust/data privacy interface. The proposal is premised on wisdom from other, more established doctrinal intersections with antitrust law. Where claims of legitimate, but conflicting, data privacy and competition interests are made, this proposal calls for both doctrines to be treated as relevant in determining the scope of permitted conduct. Neither privacy nor competition is presumed to have primacy. Instead, this approach evaluates the importance of the interests at stake in each area of law with reference to the specific conduct and context of the case. This proposal corrects for early indications that competition may be granted automatic primacy over data privacy. Instead, this proposal offers a more nuanced analysis of the new antitrust/data privacy interface that befits its importance to the digital economy.

Erika M. Douglas is an Assistant Professor of Law at Temple University, Beasley School of Law.