# Data Privacy and Antitrust in Comparative Perspective

Salil K. Mehra†



## Introduction

The current tension between the United States (U.S.) and the European Union (EU) competition law communities regarding online platforms is high and rising, particularly regarding Google and Facebook.[1] The higher scrutiny seen in the EU has focused on a myriad of issues, ranging from allegations that market power has been leveraged in ways that harm competition, to the undisclosed use of user data.[2] This tension is exacerbated by the economic salience of the "FAANG" (Facebook, Amazon, Apple, Netflix and Google) firms, several of which are in the European Commission's crosshairs.[3] All of the firms, together with Microsoft—an earlier flashpoint of regulatory tension between the U.S. and the EU—are U.S.-based and highly ranked among the world's most valuable firms.[4]

---

† Charles Klein Professor of Law, Temple University, James E. Beasley School of Law, Philadelphia, USA, smehra@temple.edu. This Article was prepared for the *Cornell International Law Journal*'s March 2019 Symposium, titled "Law's New Frontier: Cybersecurity, Privacy and Online Expression."

1. *See generally* John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PA. L. REV. 149 (2015) [hereinafter *Antitrust in Zero-Price Markets: Foundations*].

2. Ryan Browne, *Europe's Privacy Overhaul Has Led to $126 Million in Fines—But Regulators Are Just Getting Started*, CNBC (Jan. 19, 2020, 7:02 PM), https://www.cnbc.com/2020/01/19/eu-gdpr-privacy-law-led-to-over-100-million-in-fines.html [https://perma.cc/A7MN-WU2N] (reporting on fines for nonconsensual use of user data); Adam Satariano, *Facebook Loses Antitrust Decision in Germany over Data Collection*, N.Y. TIMES (June 23, 2020), https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html [https://perma.cc/7JXB-VXAY] (reporting that Facebook lost the appeal to a German court's decision that found it had violated competition law by abusing its "dominance" in user data collection).

3. Jason Fernando, *FAANG Stock*, INVESTOPEDIA (Jan. 24, 2020), https://www.investopedia.com/terms/f/faang-stocks.asp [https://perma.cc/533V-63DT].

4. *Id.*

In an era of rising nationalism, it has been tempting for U.S. observers to see the shadows of protectionism lurking behind the comparatively more stringent EU regulation of these U.S. firms. However, a more charitable explanation becomes evident: the EU embraces the concept of consumer data as property via the General Data Protection Regulation (GDPR) and other provisions, and the American absence of such a regime makes privacy and consumer data, such as competition regulation, almost unavoidable regulatory concerns for the EU. As American commentators continue to doubt whether privacy is correctly an antitrust or even a consumer protection concern,[5] American firms that build their business models on the strategic use of consumer data will likely run into tension with the EU's mode of regulation. In particular, firms that offer consumers services for their private data, then mine that data to target offers or firms that model consumers' behavior, will encounter some level of regulatory whipsaw.

This Article, prepared in connection with a symposium on cybersecurity, privacy, and online expression, explains how the tension in approaches to privacy affects the dynamics between privacy and competition law. Specifically, it sketches out three possibilities for the future: regulatory conflict, firms that reconfigure their business model to deal with an emerging "Splinternet," and some degree of harmonization between the U.S. and the EU[6]

The rest of this Article proceeds in two parts. Part I explains three prominent ways in which privacy presents an antitrust issue. Part II discusses the European GDPR in law and economics terms consonant with antitrust analysis, and explains why, as a legal development with no current U.S. analogue, the GDPR can be expected to produce tensions in antitrust enforcement.

## I. Privacy and Competition Law

Issues of competition law and privacy have quickly become closely linked. A decade ago, when the relationship of competition law and privacy first came to the forefront of legal debate, this link was hotly contested.[7] To the extent that any consensus quickly emerged, it was that

5. *See infra* Part II.

6. *See* L.S., *What is the "Splinternet"?*, ECONOMIST (Nov. 22, 2016), https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [https://perma.cc/8MVL-XHJP] (defining and discussing the concept of the "splinternet").

7. *See also* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 122–23 (2015) (arguing for a function-based distinction, and a remedy-based distinction, between privacy as an antitrust concern versus as a consumer protection concern). *Compare* Google/DoubleClick, F.T.C. File No. 071-0170 (2007) [hereinafter Google/DoubleClick] (Harbour, P.J., dissenting) (asserting lack of due consideration paid to merger's impact on the privacy concerns of consumers), *with* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1129 (2013) (arguing that several concerns, including injecting subjective notions of privacy into antitrust analysis, counsel against making consumer privacy an antitrust concern).

privacy was a non-price dimension of competition.[8] Still, a debate remained about whether antitrust law could handle privacy—with some arguing the antitrust cure might be worse than the eroded privacy disease.[9] However, changes in technology and social media business models have laid bare the links between privacy and antitrust.[10]

A. Privacy as Non-Price Competition

The point regarding the antitrust-privacy relationship that garners the greatest consensus is that consumer privacy can be a significant dimension of non-price competition.[11] Even authors who doubt the wisdom of an aggressive antitrust stance regarding privacy considerations acknowledge that privacy can form part of the bundle that consumers purchase, thus becoming a competitive factor.[12] Accordingly, antitrust consideration of privacy makes sense in theory, though applying an antitrust lens to privacy, like other qualitative factors, may be less straightforward in practice than applying it to prices and quantities.

For a long time, antitrust action was hampered by the claim that many platforms offered "free" services, and thus could not harm consumers.[13] This claim first came to prominence in connection with the *Microsoft* antitrust case, in which some argued that consumers could not be harmed because they were receiving "free" software in the form of Microsoft's Internet Explorer web browser.[14] Whatever the validity of the argument that "free" equated with no consumer harm in the landmark *Microsoft* litigation, it does not withstand scrutiny in connection with the business models employed by Amazon, Facebook, Google, and others today.[15] In these business models, consumers do not receive "free stuff," but instead

8. *E.g.*, Ohlhausen & Okuliar, *supra* note 7, at 150–51.

9. *See* D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1130, 1145 (2016) (questioning "whether current antitrust tools and policy are adequate to deal with a Big Data 'challenge,'" arguing that "harm to privacy does not, without more, equal harm to competition," and stating that "[t]he major data issues are thus not antitrust issues at all!").

10. *Id.* at 1139–40.

11. *See* Google/DoubleClick, *supra* note 7; Ohlhausen & Okuliar, *supra* note 7, at 134.

12. *See* Cooper, *supra* note 7, at 1137; Sokol & Comerford, *supra* note 9, at 1132–33.

13. *See* Joe Kennedy, *The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown*, INFO. TECH. & INNOVATION FOUND. 1, 25 (2017), http://www2.itif.org/2017-data-competition.pdf [https://perma.cc/5QH8-V5TK] (arguing against antitrust action because "many data-rich companies offer free or low-cost services that are extremely valuable to billions of people, most of whom have a pretty good idea of what data they are providing companies and how it might be used.").

14. *See* J. Gregory Sidak, *Do Free Mobile Apps Harm Consumers?*, 52 SAN DIEGO L. REV. 619, 625 (2015) (answering the title question negatively by applying the *Microsoft*-related framework and arguments to the Google/Android case). *See generally* Richard Blumenthal & Tim Wu, *What the Microsoft Antitrust Case Taught Us*, N.Y. TIMES (May 18, 2018), https://www.nytimes.com/2018/05/18/opinion/microsoft-antitrust-case.html [https://perma.cc/4ZPR-U2AL] (recapping and critiquing that argument, among others).

15. *See Antitrust in Zero-Price Markets: Foundations*, *supra* note 1, at 151–52 (deconstructing the "free" argument in antitrust); John M. Newman, *The Myth of Free*, 86 GEO.

"pay" with their personal data.[16] In a series of articles, John Mark Newman pointed out the weaknesses in antitrust reticence regarding such transactions.[17] In particular, he makes the point that antitrust can and should adapt to non-monetary payment, or else risk enabling significant consumer harm through inaction.[18]

In fact, platform business models can be more complicated than personal data-for-services exchanges because consumers may receive privacy commitments in addition to the service they buy with their personal data.[19] A recent action by the German Federal Cartel Office (FCO) against Facebook exemplifies this.[20] In its decision, the FCO prohibited Facebook from further processing user data it had generated from third-party data sources, particularly companies that had integrated "Facebook Business Tools" in their applications, until and unless Facebook obtained users' consent as set out in the EU's GDPR.[21]

While the decision was not met with universal acclaim,[22] it substantially tracks the understanding of privacy as an element of non-price competition, and the commitments to privacy as a received, or relied-on, element of the bundle that consumers purchase with their personal data. The FCO's decision found that Facebook had a "dominant position" (akin to "market power" in U.S. antitrust law) "in the German market for social networks," and that combining data from third-party apps without user consent was an abuse of this power.[23] This was because, in the FCO's view, "[d]ue to the combining of the data" with Facebook's own data, "individual data gain a significance the user cannot foresee."[24] Additionally, the FCO prohibited Facebook from cutting off users if they do not give Facebook future affirmative consent to third-party data use.[25] Notably, the decision does not punish exploitative or coercive terms per se nor impose

---

WASH. L. REV. 513, 515 (2018) [hereinafter *The Myth of Free*] (discussing the "free" argument regarding current data-based platform models).

16. *Antitrust in Zero-Price Markets: Foundations*, *supra* note 1, at 152.

17. *See generally id.*; *The Myth of Free*, *supra* note 15.

18. *See The Myth of Free*, *supra* note 15, at 583–84.

19. *Id.* at 563.

20. *See Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources Background Information on the Bundeskartellamt's Facebook Proceeding*, BUNDESKARTELLAMT 1, 1 (2019) [hereinafter BUNDESKARTELLAMT], https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?blob=publicationFile&v=5 [https://perma.cc/5FRV-3AJR] (reporting on the FCO action).

21. *Id.* at 2.

22. *See* Thibault Schrepel & John Newman, *The Bundeskartellamt's Facebook Decision: Good, Bad, and Ugly*, LECON CONCURRENTIALISTE (Feb. 11, 2019), https://leconcurrentialiste.com/2019/02/11/bundeskartellamt-facebook/ [https://perma.cc/327K-PTZC].

23. Ecem Susoy Uygun, *Germany: Germany's Federal Cartel Office Prohibits Facebook from Combining User Data from Different Sources*, MONDAQ (Mar. 19, 2019), https://www.mondaq.com/germany/data-protection/791408/germany39s-federal-cartel-office-prohibits-facebook-from-combining-user-data-from-different-sources [https://perma.cc/ES8M-65W4].

24. *See* BUNDESKARTELLAMT, *supra* note 20, at 5.

25. *Id.* at 1.

restrictions on Facebook's use of data that its own service generates.[26] Thus, the decision can be read as, in part, based on preventing a firm with significant market power from *using that power* to impose "exploitative business terms" on consumers,[27] including those that reduce privacy as a non-price element of the bundle that consumers purchase from Facebook with their attention and data.[28]

The combination of data-driven business models and privacy legislation suggests that the number of legal cases involving privacy is likely to multiply. Particularly where privacy is an element of the purchased bundle, or a dimension of competition, antitrust cases, specifically, should also increase. To the extent that privacy standards diverge between jurisdictions—particularly in the U.S. and the EU—a difference in antitrust enforcement may result.

### B. Privacy as Enabling Price Discrimination

A second potential antitrust concern regarding privacy is consumer price discrimination (sometimes referred to as individualized pricing).[29] The possibility of engaging in consumer price discrimination strongly depends on the available data about consumers with which to distinguish where on the demand curve the consumer sits.[30] While current antitrust enforcement does not emphasize action against it, price discrimination is pervasive. Even where sellers do not literally charge different prices to different buyers for substantially the same good or service (e.g., airline tickets, university educations, and new cars), they use other methods to effectively charge different prices to buyers whose willingness to pay differs.[31] Such methods include versioning (i.e., hardback vs. trade paperback vs. pocket paperback books); windowing (i.e., theatre vs. DVD vs. streaming); and two-part tariffs (i.e., cheap inkjet printers with expensive cartridges that effectively charge high-intensity users more).[32]

The Chicago School's antitrust antipathy toward prohibitions against price discrimination reflects concerns about administrability and institutional competence.[33] To address consumer welfare, the Chicago School counsels that antitrust should focus on practices that are privately beneficial but socially harmful. The pervasiveness of price discrimination sug-

26. *Id.* at 2.
27. *Id.* at 6.
28. *Id.* at 1.
29. *Cf.* TIMOTHY VAN ZANDT, FIRMS, PRICES, AND MARKETS 168–69 (INSEAD 2006).
30. *Id.* Traditionally, price discrimination also depends on the seller's ability to prevent being undercut vis-à-vis the higher-price/higher-value consumers either by competing sellers, or by arbitrage from low to high-price/high-value consumers. *Id.*
31. *Id.* at 168, 170–71.
32. *Cf. id.* at 170–71. *See* Robert A. Lawson & Ann Zerkle, *Price Discrimination in College Tuition: An Empirical Case Study*, J. ECON. FIN. EDUC., Summer 2006, at 1, 1–2; Nigel F. Piercy et al., *Thinking Strategically About Pricing Decisions*, J. BUS. STRATEGY, Sept. 2010, at 38, 41; Sofronis K. Clerides, *Book Value: Price and Quality Discrimination in the U.S. Book Market*, 1, 7 (U. Cyprus, Discussion Paper 99-15, 1999).
33. *See* William H. Page, *The Chicago School and the Evolution of Antitrust: Characterization, Antitrust Injury, and Evidentiary Sufficiency*, 75 VA. L. REV. 1221, 1254 (1989).

gests, at least, that it benefits sellers privately. The overall welfare effects of price discrimination are ambiguous. The classic example of perfect, or first-degree, price discrimination by a monopolist is not only socially beneficial, but it is also socially optimal as perfect competition.[34] However, it is generally thought not to exist in the real world, thus imperfect price discrimination involves some consumers getting better prices than others, and a transfer from consumers to sellers.[35] Effects like these make price discrimination unpopular with consumers.[36] But, by themselves, these effects do not necessarily equate to a loss of social welfare. That said, imperfect price discrimination—the kind that is more likely to occur in reality—does tend to lead to reduced output, and therefore deadweight loss,[37] at least vis-à-vis a theoretically competitive market with a single price. As a result, price discrimination could be seen as a socially harmful practice that is privately beneficial, and therefore a target of antitrust policy.

However, government antitrust enforcement has not made price discrimination a prime target. This is a direct result of the Chicago School antipathy rooted in questions about market power and incentive effects, a hangover from antitrust's much-maligned Robinson-Patman Act, and the difficulty in the practice of identifying price discrimination.[38]

First, due to the possibility of competitive response, the ability of a seller to sustainably price discriminate usually means that that firm already has market power; price discrimination simply allows it to earn more from market power than it already possesses. To the extent that market power has been obtained without predation or exclusion, and instead represents returns to innovation or aggressive competition, concerns arise about the incentive effects of punishing price discrimination. Additionally, since trying to discern consumers' willingness to pay takes effort and creates costs, even firms with market power may be dissuaded from undertaking price discrimination strategies.

---

34. *See* Thierry Rayna et al., *Pricing Music Using Personal Data: Mutually Advantageous First-Degree Price Discrimination*, 25 ELECTRONIC MKT. 139, 144–45 (2015). It does, however, have strikingly different distributional results.

35. *See* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, PROC. FIFTH INT'L CONF. ON ELECTRONIC COM. 355, 357 (2003) (suggesting that unpopularity of price discrimination with the public will limit it or force it to take subtler or hidden forms).

36. Akiva A. Miller, *What Do We Worry About when We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 41, 88 (2014) (stating that "[t]he public's dislike of unfairness, even in the face of other benefits, is likely to be a powerful factor that will limit the spread of price-discrimination strategies."). *See also* Odlyzko, *supra* note 35, at 358–59.

37. Deadweight loss is a loss of produced output that causes lost consumer and producer surplus. *See* Raymond Chiang & Chester S. Spatt, *Imperfect Price Discrimination and Welfare*, 49 REV. ECON. STUD. 155, 169 (1982). *See, e.g.*, HERBERT HOVENKAMP, FEDERAL ANTITRUST POLICY 772 (West Academic Publ'g 5th ed. 2016); Dennis W. Carlton, *Roundtable on Price Discrimination*, ORG. ECON. CO-OPERATION & DEV. 1, 5 (2016) (background note for the Organisation of Economic Co-operation and Development (OECD) Competition Committee giving examples of how imperfect price discrimination can be efficient or inefficient).

38. Terry Calvani & Gilde Breidenbach, *Introduction to the Robinson-Patman Act and Its Enforcement by the Government*, 59 ANTITRUST L.J. 765, 773 (1991).

Second, for the past few decades, most of the antitrust community has lived in an uneasy tension with the Robinson-Patman Act,[39] which punishes a subset of price discrimination in a manner that cannot easily be reconciled with consumer welfare. Instead, the Act seems to reflect distributional concerns, such as preserving smaller retailers.[40] Antitrust efforts aimed at price discrimination may have suffered from a kind of guilt by association.

Finally, trying to punish socially harmful price discrimination implies assessing the social welfare impacts of different prices on different groups. This is potentially a very complex task, especially if the price discrimination involves aspects other than, or in addition to, a uniform good at different prices.[41]

However, changed circumstances make us wonder about the existing consensus on price discrimination. Specifically, the ability to gather data on individual consumers, process it algorithmically, and set prices automatically, has driven Silicon Valley to invest in technologically oriented economists in order to develop and spread price discrimination strategies.[42] As a result, price discrimination may become more widespread, and its effect may be qualitatively different.[43]

Changes in the underlying technologies and policy responses could require a reevaluation of price discrimination. A newly technology-enabled pricing algorithm "may serve to promote [instances of] price discrimination that can either raise or lower social welfare."[44] This new reality relates to a key point of dispute at the dawn of the Chicago School antipathy. Richard Posner had claimed that, because price discrimination makes monopoly more profitable by transferring consumer surplus to the monopolist, firms would make additional investments to gain monopolies, result-

39. *See* Richard M. Steuer, *Crossing the Streams of Price and Promotion Under the Robinson-Patman Act*, ANTITRUST, Fall 2012, at 64, 64 (observing that "[d]espite all the criticism that has been heaped upon the Robinson-Patman Act since its enactment, and all the efforts at repeal, it appears that the Act will remain in effect as long Congress continues to believe that small dealers need special protection to gain traction and survive in competition against larger rivals.").

40. *See* Coastal Fuels v. Caribbean Petroleum Corp., 79 F.3d 182, 192 (1st Cir. 1996) (discussing the legislative history of the Robinson-Patman Act and declining to extend the *Brooke Group* standard—concerning harm by a seller to its competitor—to price discrimination by a seller that harms some downstream buyers vis-à-vis others).

41. *See* Carlton, *supra* note 37, at 6.

42. Jerry Useem, *How Online Shopping Makes Suckers of Us All*, ATLANTIC (May 2017), https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/ [https://perma.cc/6SU6-ZUAB] (describing economists working for Silicon Valley firms as involved in experiments aimed at using Big Data to "discern every individual's own *personal* demand curve" and thus estimating willingness to pay in order to price discriminate).

43. *See* Terrell McSweeney & Brian O'Dea, *The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement*, ANTITRUST, Fall 2017, at 75, 75 (demonstrating with examples how "increasingly sophisticated price discrimination may lead to narrower relevant product markets, potentially increasing the chances that a merger will harm consumers in some relevant markets.").

44. Joseph E. Harrington, Jr., *Developing Competition Law for Collusion by Autonomous Artificial Agents*, 14 J. COMPETITION L. & ECON. 331, 351 n.37 (2019).

ing in socially wasteful investments.[45] Robert Bork countered Posner's observation saying that it "seem[ed] less an objection to permitting a monopolist to maximize his revenues through price discrimination than an additional reason to object to the achievement of monopoly" through means other than "ways of which antitrust approves," such as obtaining a patent or increased cost efficiency.[46]

Posner's argument now has new bite to the extent that firms have been deploying emerging technologies that gauge consumers' willingness to pay and defeat consumer arbitrage.[47] Such investments may include lobbying governments to make such data collection easier, which may be exactly what antitrust should aim to deter—actions that are privately optimal to the firm but socially harmful, and which may result in cases where the wealth transfer from consumers to producers (e.g., a social wash) outweighs the investment in price discrimination (e.g., a social loss).[48] Moreover, in the online context, firm investments in data gathering may result in consumer investments in privacy—and a costly arms' race may ensue.[49]

Preventing such an inefficient arms race could emerge as a legitimate objective of competition law enforcement involving privacy. While some may argue that other avenues of law could fit better, that is essentially an argument about the relative capacity of institutions and doctrines as they exist. Where institutions and doctrines differ, for example, between the U.S. and the EU, we may expect tensions in antitrust enforcement regarding privacy.

### C. Privacy and Consumer Data as an Entry Barrier

A third way in which privacy can become an antitrust concern is if the acquisition of consumer data by an incumbent firm becomes a barrier to

45. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 127 (Little, Brown & Co. 1st ed. 1972).

46. ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF 396 (Basic Books, Inc. 1978).

47. Oren Bar-Gill, *Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)perceptions*, 86 U. CHI. L. REV. 217, 225–27 (2019) (describing firms' use of various indicators to gauge willingness to pay).

48. POSNER, *supra* note 45, at 127 (pointing out that price discrimination makes monopolies more profitable by transferring consumer surplus to the monopolist; therefore, firms could invest in monopolies, but these investments would be socially wasteful).

49. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009 (2013). Examples of this "arms-race" dynamic include the history of digital rights management software and the work of those who circumvent such technology, as well as the history of combatting online file-sharing and false speech online, *see* Abbas Foroughi et al., *Digital Rights Management: A Delicate Balance Between Protection and Accessibility*, 28 J. INFO. SCI. 389, 390 (2002); Christopher M. Swartout, *Toward a Regulatory Model of Internet Intermediary Liability: File-Sharing and Copyright Enforcement*, 31 NW. J. INT'L L. & BUS. 499, 504, 506 (2011); Richard M. Schmidt, Jr. & Robert Clifton Burns, *Proof or Consequences: False Advertising and the Doctrine of Commercial Speech*, 56 U. CIN. L. REV. 1273, 1289–90 (1988).

enter the market.[50] While antitrust implications are often discussed under the broader umbrella term "Big Data," the relevant subcategory is often a large-scale gathering of private consumer information. A key factor is that the mosaic produced by data obtained from a myriad of individuals, not only produces insights about those individuals' preferences, but can also generate value greater than the sum of its parts by revealing market insights about collective behavior.[51]

Mass collection of consumer data could produce entry barriers germane to several antitrust contexts. Hypothetically, incumbents could use a "Big Data"-related advantage to provide defensive leverage against a new insurgent firm or to favor their own products in new markets via exclusionary conduct.[52] Because of the novelty of such issues, we cannot yet critique whether the facts of such cases would adequately support antitrust intervention against such alleged conduct.

The antitrust context in which consumer data collection has probably received the most scrutiny is merger review—specifically, Facebook's acquisitions of Instagram and WhatsApp. In 2012, Facebook's acquisition of Instagram was cleared relatively easily.[53] While the Federal Trade Commission (FTC) also cleared Facebook's acquisition of WhatsApp in 2014, it did notify Facebook that it would have to honor WhatsApp's privacy commitments to users notwithstanding the acquisition.[54] Although this could be seen as a form of consumer protection—requiring a firm's acquirer to honor previously made commitments—it also discourages merging to prioritize retroactive reduction of competition over privacy commitments to users.[55]

In the intervening years, a significant debate emerged about the degree to which the FTC correctly analyzed Facebook's acquisitions, and, more

50. *See* Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 369–70 (listing observations relevant to whether data collection is likely to be an entry barrier to new competitors).

51. *Id.* at 379.

52. *Id.* at 370.

53. *See* Press Release, Fed. Trade Comm'n, FTC Closes Its Investigation into Facebook's Proposed Acquisition of Instagram Photo Sharing Program (Aug. 22, 2012) (available at https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition [https://perma.cc/49QM-2FLB]) (reporting a five to zero Commission vote to "close its nonpublic investigation . . . without taking any action.").

54. Press Release, Fed. Trade Comm'n, FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition (Apr. 10, 2014) (available at https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition [https://perma.cc/U9DA-2PC5]) (clarifying that "WhatsApp must continue to honor these promises to consumers" or else "both companies could be in violation of Section 5 of the [FTC] Act.").

55. *See* Charles McConnell, *McSweeny: Privacy Competition Standard Could Have Sunk Facebook/WhatsApp*, GLOBAL COMPETITION REV. USA (Sept. 29, 2017), https://globalcompetitionreview.com/article/usa/1147829/mcsweeny-privacy-competition-standard-could-have-sunk-facebook-whatsapp [https://perma.cc/79YK-AXFU] (interviewing then-FTC commissioner who stated that these commitments were actually not kept post-merger, and that antitrust and the protection of consumer privacy can be intertwined—particularly, in the merger context).

specifically, whether antitrust policy has properly reflected the advantages firms garner from mass consumer data collection.[56] In addition to inhibiting entry, Tim Wu has described these advantages as promoting "the Kronos Effect."[57] Named after a Greek god who devoured his children, the Kronos Effect represents "the efforts undertaken by a dominant company to consume its potential successors in their infancy."[58] Such concerns align with observations that new entrants now avoid what they call the "kill zones" of Amazon, Facebook, and Google—that is, "the areas in which they are capable of crushing any competition."[59] And since "[b]reakthrough ideas often come from startups rather than from large firms, [ ] this could be depriving us of important innovations."[60]

## II. Consumer Data, Privacy Regulation, and Antitrust

Due to the increasing salience of business models built on gathering massive amounts of consumer data, antitrust enforcement will likely continue to confront privacy issues. As a non-price competitive dimension, in connection with price discrimination, or as an entry barrier, consumers' privacy interests will determine how antitrust enforcement construes and handles claims built on these theories. But the definition of consumers' privacy interests will also matter. An increasing source of tension between U.S. and EU antitrust approaches may emerge in the form of divergent privacy regulation.

### A. Consumer Data and Privacy Regulation

How to govern consumer data has been a topic of debate since the early days of what was then referred to by now-quaint names such as "Cyberspace" and the "World Wide Web."[61] Clearly, different levels of protection for consumer privacy are emerging on each side of the Atlantic. Simply put, there is no U.S. equivalent to the EU's GDPR.[62]

---

56. *See* Rubinfeld & Gal, *supra* note 50, at 369–70 (listing considerations). *Compare* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 286 (Oxford Univ. Press 1st ed. 2016) (claiming that the "data-opoly can use its relative advantage" and "acquire entrants before they become significant competitive threats or blunt the entrant's growth (such as manipulating its search engine results to make it harder to find the company)."), *with* D. Daniel Sokol & Roisin Comerford, *Does Antitrust Have a Role to Play in Regulating Big Data?*, *in* THE CAMBRIDGE HANDBOOK OF ANTITRUST, INTELLECTUAL PROPERTY AND HIGH TECH 293, 313 (Roger D. Blair & D. Daniel Sokol eds., Cambridge Univ. Press 2017) (arguing that "[t]he existing theories of harm conflict with the realities of Big Data (e.g., nonrivalrous, ubiquitous, low barriers to entry. . .).").

57. TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 25 (2010).

58. *Id.*

59. Martin Giles, *It's Time to Rein in the Data Barons*, MIT TECH. REV. (Jun. 19, 2018), https://www.technologyreview.com/s/611425/its-time-to-rein-in-the-data-barons/ [https://perma.cc/86RS-VJF6].

60. *Id.*

61. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 102, 159–63 (Basic Books, Inc. 1999).

62. Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/

While a thorough review of the GDPR is beyond the scope of this Article, it can be seen as the culmination of a two decade-long discussion on how to handle online privacy. Perhaps the first prominent proposal was by Lawrence Lessig, who considered how to handle the sharing of personal data across websites. In the late 1990s, he advocated for a system in which rights to personal data would be allocated to users like property.[63] Users would then transact with websites via software protocols that would manage or restrict the use of their data.[64] Embedded in this regime was the conception of "cyberspace" as a world with minimal transaction costs, resembling the world of the Coase theorem, in which all that was needed was clear property rights since voluntary transactions could then achieve the efficient result.[65]

In contrast to Lessig's distinctly Coasean vision, Paul Schwartz advocated for a mixed-property liability regime.[66] Like Lessig, Schwartz' proposal would involve allocating users with property rights to their personal data.[67] However, unlike Lessig's, it would also involve restrictions that "run with" that property right even after the transfer, particularly the right to block further transfers of personal data beyond the initial one.[68] Such right could be waived, but only with affirmative consent.[69] Schwartz's regime drew on the landmark work of Guido Calabresi and Douglas Melamed, which counseled for property rules with few obstacles in order to facilitate voluntary cooperation between parties, and liability rules where such obstacles do exist.[70] Schwartz saw user privacy as demanding a degree of restriction on inalienability, but not enough to prevent some trade in personal data—hence, the hybrid regime.[71]

---

news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/ [https://perma.cc/QKE9-9PZY] (observing that "there's no equivalent of the GDPR in the United States, nor is there likely to be one anytime soon. A mosaic of different state and federal rules, some of them varying widely, govern some of the same issues, but there's no central authority that enforces them.").

63. *See* LESSIG, *supra* note 61, at 159–63.

64. *Id.*

65. *Id.*

66. Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices,* 2000 WIS. L. REV. 743, 745 (2000) [hereinafter *Beyond Lessig's Code for Internet Privacy*] (arguing that the "Calabresi-Melamed [ ] framework adopted by Lessig points not to the merits of a pure property solution, but to the benefits of a mixed property-liability regime."); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2060 (2004) [hereinafter *Property, Privacy, and Personal Data*] (proposing a "model of propertized personal data involv[ing] the development of a hybrid inalienability consisting of a use-transfer restriction plus an opt-in default" in which the "ability to block [further transfers of data beyond the initial one] will generally be set as an opt-in, which means that further use or transfer will not be allowed unless the individual affirmatively agrees to it.").

67. *See Property, Privacy and Personal Data*, *supra* note 66, at 2058.

68. *Id.*

69. *See id.* at 2098.

70. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral,* 85 HARV. L. REV. 1089, 1092, 1126 (1972).

71. *See Property, Privacy and Personal Data*, *supra* note 66, at 2094–97.

Arguably, with the GDPR, the EU has adopted something resembling Schwartz's hybrid regime.[72] The GDPR gives "consumers . . . clear entitlements to their own data; the data, even after it is transferred, carries. . . [restrictions] that 'run[ ] with' it and bind[ ] third parties; and consumers are protected" with affirmative remedies for violations.[73] By contrast, the closest thing to the GDPR in the U.S. may be the California Consumer Privacy Act of 2018 (CCPA).[74] However, the CCPA has not been implemented yet, and it faces pending federal legislation to overrule it.[75] Moreover, even if the CCPA were to survive, it would be complicated to use it as a baseline to understand privacy issues germane to *federal* antitrust law. Accordingly, at least for the foreseeable future, the GDPR represents a significant difference in the understanding of privacy norms and expectations between the U.S. and the EU.

### B. The Antitrust Impact

As discussed in Part II above, privacy can be an antitrust concern, whether as a producer's non-price output, as a price-discriminator's input, or as an entry barrier to new competition. Because of the current transatlantic divergence in privacy protection, each of these three examples of privacy-antitrust issues can lead to antitrust divergence. Interestingly, this divergence could take different forms depending on the nature of the antitrust concern involved.

First, where privacy is a non-price dimension of competition, antitrust enforcement could result in tension over whether or not injury to competition from certain conduct or merger actually exists. To conclude that a consumer's ability to protect their privacy has been harmed requires a definition of what consumer data should be protected by rights to privacy. Moreover, without a conception rooted in something like the GDPR allowing consumers to exercise sovereignty over their personal data, a con-

72. Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 515 (2013) (highlighting several elements of the GDPR that are "remarkably similar to existing, heretofore purely theoretical, proposals for property regimes for protecting personal data, especially the model proposed by Paul Schwartz in 2004.").

73. *Id.*

74. Susan Okin Goldsmith et al., *Surf's Up– California Introduces the Next Wave of the Data Privacy Revolution*, MCCARTER & ENG. LLP (Feb. 26, 2019), https://www.mccarter.com/insights/surfs-up-california-introduces-the-next-wave-of-the-data-privacy-revolution/ [https://perma.cc/NE6V-CVJQ] (describing the CCPA as the "first-of-its kind data privacy law in the United States" and comparing specific provisions to those of the GDPR); Etelka Lehoczky, *California is Bringing E.U.-Style Privacy Laws to the U.S. Here's What You Need to Know*, INC., https://www.inc.com/magazine/201902/etelka-lehoczky/california-privacy-law-gdpr-compliance-customer-data-rights.html [https://perma.cc/4SSG-4BK6].

75. Kiran Stacey, *Silicon Valley Lobbies Hard to Kill Off California Privacy Rules*, FIN. TIMES (Mar. 5, 2019), https://www.ft.com/content/c3746540-3f57-11e9-b896-fe36ec32aece [https://perma.cc/5TDU-VTDJ] (reporting that "[t]ough new data privacy rules in California" that "contain[ ] similar provisions to the EU's General Data Protection Regulation" could be "overruled before they are even implemented" through pending federal legislation).

duct or merger that erodes consumers' ability to govern their data might not be viewed as significant enough to merit anti-competitive concern. In the context of non-price competition, differing underlying notions of privacy could yield different outcomes even when using similar antitrust methods.

Second, where consumer price discrimination is viewed as an antitrust concern, privacy protection could lead to a form of antitrust "Splinternet." To the extent that the GDPR prevents the collection of consumer data necessary to accomplish sophisticated price discrimination—and that the lack of similar legislation in the U.S. fails to prevent that data collection—we could see advanced forms of price discrimination, or individually targeted offers, emerge in the U.S. and not in the EU. As a result, depending on the reception of U.S. antitrust authorities to price discrimination-based theories of consumer harm, we could see the development of a price discrimination antitrust regime in the U.S. without an EU analogue.

Finally, gathering of consumer data as an anti-competitive barrier to entry could yield a degree of harmonization. There is no area of antitrust law with more effort toward harmonization, competition agency investment, and concrete results than merger review. Regarding mergers of transnational firms, antitrust agencies in the U.S. and the EU already consider the competitive impacts of activities outside their own territory.[76] As a result, the ability of consumer data collection to serve as a barrier to entry can be a source of antitrust action even where that data collection takes place abroad. Accordingly, it would not be surprising to see agreement between U.S. and EU approaches to data-related mergers—not just generally, but also in specific cases—since the source of the entry barrier need not necessarily matter to the enforcer.

**Conclusion**

Despite some differences, antitrust approaches on both sides of the Atlantic are characterized by a high degree of harmonization. However, a significant gap has developed in understanding consumer privacy, at least if legislative protection is used as a baseline. Due to the increasing importance of consumer data gathering to contemporary business models, consumer privacy will likely become a relevant antitrust consideration, at least in the facets discussed, but likely, in other aspects as well. As a result, some divergence in cross-Atlantic antitrust enforcement is also possible given the disparate approaches to privacy.

76. Pinar Karacan, *Differences in Merger Analysis Between the United States and the European Union, Highlighted in the Context of the Boeing/ McDonnell Douglas and GE/ Honeywell Mergers*, 17 GLOBAL BUS. & DEV. L.J. 209, 210 (2004) (observing that "[t]he European Merger Regulation is applied extraterritorially when the merger is above a certain threshold" and that "[s]imilar to Europe, the United States applies its competition laws to foreign companies based on the 'effects test,'" which looks at the activity's impact on the U.S. even if it is outside U.S. borders).