VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2020 UNIVERSITY OF VIRGINIA VOL. 24, NO. 2

Monopolization Remedies and Data Privacy

ERIKA M. DOUGLAS†

† Assistant Professor of Law, Temple University, Beasley School of Law.

For their thoughtful input on this article, I would like to thank A. Douglas Melamed, Salil K. Mehra, Bruce E. Boyden, Jonathan Smollen, Rachel Rebouché, Jim Gibson, Kristen Osenga, Spencer Weber Waller, my Temple University colleagues and participants in the Richmond University Junior Faculty Forum, the Arizona State University Sandra Day O'Connor College of Law Governance of Emerging Technology & Science and the Marquette Junior Faculty Forum. All errors and omissions are my own.

ABSTRACT

As one former agency head explains, antitrust litigation is like fishing: "everybody likes to catch them, but nobody wants to clean them." Antitrust enforcers around the world are eager to catch digital platforms with monopolization cases, but little attention is being paid to the remedies that will follow.

This article examines a new source of complexity for those monopolization remedies—data privacy. In particular, it considers remedies that require access to, or disclosure of the information held by digital platforms, to restore online competition. How are such "data access" remedies impacted by the rise of consumer data privacy law?

As the article explains, neither current theory nor past monopolization cases answer this question. Existing theories on the interface between antitrust law and data privacy are focused on liability. Their application may therefore miss the distinct privacy impacts that arise at the remedies stage of a case. Past monopolization cases that ended in data access remedies often ordered disclosure of company, not consumer, information. Individual data privacy was simply not relevant. The rare historical cases that ordered disclosure of consumer information pre-date the rise of U.S. data privacy law from the mid-1990s to present. For the first time, antitrust remedies may well have to contend with consumer privacy protection, and the control such protection can impart over competitively important data.

The article calls for antitrust analysis to consider data privacy in the design of remedies, particularly for digital platforms. Without such analysis, remedies may unwittingly cause privacy harms that outweigh the benefits to consumers from restored competition. A remedy that causes such a reduction in consumer welfare would undermine the purpose of bringing antitrust enforcement action.

The article concludes with discussion of two potential approaches for implementing the proposal. The first focuses on obtaining consumer consent to remedial disclosure and use of data. The second focuses on legislative or judicial definitions of data privacy interests that exclude remedial disclosure. Both demand careful consideration of consumer privacy, and the new complexity it creates for monopolization relief.

TABLE OF CONTENTS

I. INTRODUCTION

The design of effective monopolization remedies poses one of the greatest challenges in modern antitrust law. This is particularly true in technology cases, where remedial design has been compared to "trying to shoe a galloping horse,"[1] "catching [a] tiger by the tail,"[2] or whopping a mule "upside the head."[3] The abundance of wild animal analogies reflects a core truth—dominant technology companies are dynamic, powerful and hard to tame.

Antitrust agencies are barreling toward this type of complex monopolization remedy with investigations of the most successful technology companies in the world. Digital platforms like Facebook, Google, Apple and Amazon[4] have found themselves under scrutiny by federal antitrust authorities,[5] fifty

---

[1] U.S. DEP'T OF JUSTICE, COMPETITION AND MONOPOLY: SINGLE–FIRM CONDUCT UNDER SECTION 2 OF THE SHERMAN ACT 158 (2008) [hereinafter DOJ SINGLE–FIRM CONDUCT GUIDELINES]. Although this guidance was formally rescinded after a change in administration, it remains a useful reflection of the law on Section 2 of the Sherman Act.

[2] Thomas O. Barnett, *Section 2 Remedies: What to Do After Catching the Tiger by the Tail*, 76 ANTITRUST L.J. 31, 31 (2009).

[3] United States v. Microsoft Corp., 253 F.3d 34, 111 (D.C. Cir. 2001).

[4] The term "digital platform" is used here to refer to large technology companies whose online products and services create value by intermediating between different groups. *See, e.g.*, Ohio v. Am. Express Co., 138 S. Ct. 2274, 2280 (2018) (discussion of two–sided platforms); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1015 (2013) (describing platforms as "connectors between users and what they want").

[5] Press Release, U.S. Dep't of Justice, Justice Department Reviewing the Practices of Market–Leading Online Platforms (July 23, 2019), https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online–platforms [hereinafter DOJ Digital Platform Investigation] ("The Department's Antitrust Division is reviewing whether and how market–leading online platforms have achieved market power and are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers."); 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 [hereinafter Fed. Trade Comm'n Task Force Press Release]. The Department of Justice Antitrust Division ("DOJ") and the Federal Trade Commission ("FTC") enforce U.S. federal antitrust law.

state attorneys general[6] and both Houses of Congress.[7] These companies also face countless investigations, suits and fines for monopolization outside of the U.S.[8] An unprecedented chorus of

[6] Tony Romm, *50 U.S. States and Territories Announce Broad Antitrust Investigation of Google*, WASH. POST (Sept. 9, 2019), https://www.washingtonpost.com/technology/2019/09/09/states-us-territories-announce-broad-antitrust-investigation-google.

[7] *Online Platforms and Market Power, Part 1: The Free and Diverse Press: Hearing Before the Subcomm on Antitrust, Commercial and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (2019); *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).

[8] DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, DISINFORMATION AND 'FAKE NEWS': FINAL REPORT, 2017–19, HC 1791, at 38 (UK) (including investigation of Facebook's alleged exclusion of competitors such as Vine, a short–format video posting app, that relies on Facebook to reach users); Press Release, Bundeskartellamt, Bundeskartellamt Initiates Abuse Proceeding Against Amazon (Nov. 29, 2018), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/29_11_2018_Verfahrenseinleitung_Amazon (investigating whether Amazon's "double role as the largest retailer and largest marketplace has the potential to hinder other sellers on its platform"); Press Release, Bundeskartellamt, Bundeskartellamt Initiates Proceeding Against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection Rules (Mar. 2, 2016), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook; 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; European Commission Press Release IP/19/429, 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 (opening an investigation into Amazon's use of "sensitive data from independent retailers who sell on its marketplace"). The European competition authorities have fined Google for abuse of monopoly three times in the span of just three years. *See* European Commission Press Release IP/19/1770, 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 (fining Google for its contracting practices in online advertising); European Commission Press Release IP/18/4581, 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 (fining Google for its restrictions on Android device manufacturers and

politicians,[9] scholars[10] and media pundits[11] have joined these efforts, calling for aggressive anti-monopolization enforcement against digital platforms.

This article examines a new source of complexity for antitrust remedies—data privacy.[12] In particular, it looks at growing calls for remedies that order access to, or disclosure of the information held by digital platforms, as a means of restoring

---

mobile network operators related to use of Google Search); European Commission Press Release IP/17/1784, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017) [hereinafter European Commission Press Release on Google Search], https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 (fining Google for preferring its own website links in search results).

[9] Sen. Elizabeth Warren, *Here's How We Can Break Up Big Tech*, MEDIUM (Mar. 8, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c (proposing structural separation for large technology platforms and non-discriminatory dealing obligations for smaller platforms); Rep. David Cicilline, The Case for Investigating Facebook, N.Y. TIMES (Mar. 19, 2019)(advocating for antitrust enforcement against Facebook).

[10] *See, e.g.*, TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018); Lina M. Khan, *The Separation of Platforms and Commerce* 119 COLUM. L. REV. 973 (2019) (proposing new antitrust controls over technology platforms like Amazon, Facebook and Google); Maurice E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, HARV. BUS. REV. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data.

[11] *See, e.g.*, Eric Posner & Glen Weyl, Opinion, *The Real Villain Behind Our New Gilded Age*, N.Y. TIMES (May 1, 2018), https://www.nytimes.com/2018/05/01/opinion/monopoly-power-new-gilded-age.html; Jeffrey Katz, *Google's Monopoly and Internet Freedom*, WALL ST. J. (June 7, 2012), https://www.wsj.com/articles/SB10001424052702303830204577448792246251470; Jonathan Taplin, *Is it Time to Break up Google?* N.Y. TIMES (Apr. 22, 2017), https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html.

[12] This article adopts a conception of data privacy as reflected in FTC enforcement. *See infra* Section III.B.1. *The Rise of Data Privacy and its Application to Digital Platforms*. It leaves aside other conceptions of privacy, such as physical space privacy or decisional privacy over bodily integrity and family. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–03 (1998) (identifying privacy as overlapping ideas of physical space privacy, choice privacy and flow of personal information).

online competition.[13] It argues that demands for such "data access" remedies raise unaddressed tension with the protection of individual data privacy.

Part I of the article introduces the law of monopolization remedies. It also explains why data access remedies are the likely outcome in impending digital platform cases, if antitrust enforcers succeed.

Part II describes the established theories on the intersection of antitrust law with data privacy. It argues that because such theories focus on liability, they may miss the distinct data privacy impacts arising at the remedies stage of a case.

Part III of the article looks at data access remedies against platforms of the past, including computing and telephone service monopolists. It finds that remedies in these historical cases had no cause to contemplate consumer privacy interests. Most older remedies involved access to company, not consumer, data. The cases that disclosed personal information largely predate the rise of U.S. data privacy law, which occurred from the mid-1990s to present. For the first time, consumer data has become both important to competition, and protected by data privacy law. This creates new challenges for the design of data

[13] *See, e.g.*, D. Bruce Hoffman, Director, Bureau of Competition, Fed. Trade Comm'n, Technology and Its Discontents: Taking Stock of Antitrust and Technological Change in the Early 21st Century, Remarks Before the Capitol Forum's Fifth Annual Technology, Media, & Telecom Competition Conference, at 13 (Dec. 13, 2018), https://www.ftc.gov/system/files/documents/public_statements/1433988/capitol_forum_remarks_bh.pdf ("[D]oes antitrust provide an answer to whatever problems may exist with the accumulation of data? Some commentators at the hearing thought the answer lay in . . . requiring firms to share their data troves."); Margrethe Vestager, Comm'r of Competition, Eur. Comm., Defending Competition in a Digitised World, Speech at European Consumer and Competition Day (Apr. 4, 2019), https://wayback.archive-it.org/12090/20200221202247/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/defending-competition-digitised-world_en ("[O]ne thing we may need to do, to open up competition, is to require companies to give rivals access to their data.").

access remedies, arising from the conception of privacy as control over information.

To address these challenges, Part IV of the article calls for antitrust analysis to consider data privacy interests in the design of remedies. It argues that without such consideration, data access remedies may unwittingly cause privacy harms that outweigh the benefits to consumers from restored competition. Such remedies would undermine the purpose of bringing antitrust enforcement action.

The article concludes with discussion of two potential approaches to implement this proposal, and the pros and cons of each. The first and most immediate possibility is to obtain consumer consent to remedial disclosure and use of data. However, as data privacy protection expands in U.S. law, this "consent-to-remedy" approach will suffer from growing tradeoffs between the protection of privacy and the design of effective and administrable remedies. The second approach is longer-term, and focuses on legislative or judicial definitions of data privacy interests that exclude remedial data disclosure. The emphasis of both approaches, and the article as a whole, is on careful thinking about the impact of data privacy on the design of digital monopolization remedies.

A. Introduction to the Law of Monopolization Remedies

It may seem odd to start at the end of a case, with remedies. But now is the time to look ahead, as potential cases against digital platforms gather momentum. The Department of Justice, Antitrust Division ("DOJ") explains that "[e]arly and careful consideration of remedies in section 2 cases is vitally important."[14] Many scholars echo this call to contemplate remedies at the outset of a monopolization case, warning that antitrust "[e]nforcers should be considering remedies from the moment an investigation is commenced."[15] Since the DOJ and

[14] DOJ SINGLE–FIRM CONDUCT GUIDELINES, *supra* note 1, at 163.

[15] Edward Cavanagh, *Antitrust Remedies Revisited*, 84 OR. L. REV. 147, 201 (2005); DOJ SINGLE–FIRM CONDUCT GUIDELINES, *supra* note 1, at 143 (reporting that panelists in hearings for the report "stressed that antitrust enforcement agencies need to give careful consideration to

the Federal Trade Commission ("FTC") have both commenced wide-ranging investigations into digital platforms, now is the time to begin thinking about appropriate remedies.[16]

Early consideration of remedies is important because it acts as a disciplining mechanism, testing the robustness and specificity of liability-stage theories. Although analytically distinct stages of a case, antitrust scholarship has long treated the questions of remedies and liability as related. Antitrust analysis "blur[s] the line" between the two, particularly for unilateral conduct.[17] As Judge Posner observes, the "nature of the remedy sought in an antitrust case is often . . . an important clue to the soundness of the antitrust claim."[18] If there is no logical remedy available for the misconduct, that may indicate the liability theory needs refinement, or even that scarce prosecutorial resources are better spent elsewhere.[19] If the case proceeds, the

---

potential remedies early in their investigations."); *id*. at 143 n.3 (quoting Sherman Act Section 2 Joint Hearing: Section 2 Policy Issues Hr'g Tr. 13, May 1, 2007 (Krattenmaker)) (explaining that "you begin with remedies" in a Section 2 Sherman Act case); *id.* (quoting Sherman Act Section 2 Joint Hearing: Section 2 Policy Issues Hr'g Tr. 13, May 1, 2007 (Baer)) (advocating "thinking about remedy . . . as a front-end issue"); *id*. (quoting Sherman Act Section 2 Joint Hearing: Section 2 Policy Issues Hr'g Tr. 13, May 1, 2007 (Shelanski)) (arguing that a remedy "needs to be clearly articulable at the start of a case"); Barnett, *supra* note 2, at 76 ("[I]t is critical to think hard about what you are going to do with the tiger before you grab its tail.").

[16] DOJ Digital Platform Investigation, *supra* note 5; Fed. Trade Comm'n Task Force Press Release, *supra* note 5.

[17] A. Douglas Melamed, *Afterword: The Purposes of Antitrust Remedies*, 76 ANTITRUST L.J. 359, 367 (2009) ("[S]ince [Donald Turner's seminal article], antitrust commentary has regularly blurred the line between liability standards and remedy. This blurring has been especially common in the context of unilateral conduct.").

[18] Brunswick Corp. v. Riegel Textile Corp., 752 F.2d 261, 267 (7th Cir. 1984).

[19] William E. Kovacic, *Designing Antitrust Remedies for Dominant Firm Misconduct*, 31 CONN. L. REV. 1285, 1310 (1999) (casting early decisions on remedies as a matter of "[r]esponsible prosecutorial practice"); DOJ SINGLE–FIRM CONDUCT GUIDELINES, *supra* note 1, at 143 n.3 (quoting Sherman Act Section 2 Joint Hearing: Welcome and Overview of Hearing, Hr'g Tr. 52-53, June 20, 2006 (Hovenkamp)) ("The only purpose in bringing [Section 2] cases is to make the economy work better, and if you do not have a clear picture of the kind of remedy you want when you go in, then you really have to wonder whether it is worth bringing the action to

willingness of a court to grant a particular remedy will depend on what is proven at the liability stage, which means the claims, arguments and evidence should be developed with the intended remedy in mind.

No particular form of relief is automatic for violations of Section 2 of the Sherman Antitrust Act (the "Sherman Act").[20] Instead, trial courts have broad discretion to order relief that will remedy the unlawful conduct.[21] In cases where the government is the plaintiff, possible remedies range from criminal penalties

---

begin with."). This article does not go so far as to contend that a case should be abandoned if the remedies are not clear at the outset. Rather, it takes the position that early thinking on remedies is productive and useful, particularly for complex unilateral conduct cases in the digital sector.

[20] PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW: AN ANALYSIS OF ANTITRUST PRINCIPLES AND THEIR APPLICATION ¶ 653a (4th ed. 2020). To obtain a remedy, the plaintiff must establish a violation of a Section 2 Sherman Act, which requires a showing that the monopolist: (1) possesses monopoly power in a relevant antitrust market and (2) willfully acquired or maintained that power (or attempted to do so), "as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident." 15 U.S.C. § 2 (2018); United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966). The first element, monopoly power, is "the power to control prices or exclude competition," such as the ability to raise prices substantially above the competitive level. United States v. E.I. du Pont de Nemours & Co., 351 U.S. 377, 391 (1956). This is typically shown through evidence that the defendant holds a high market share, and evidence on the market structure. *See, e.g.*, *Grinnell,* 384 U.S. at 571. Mere possession of monopoly power is not unlawful, meaning the second element must also be shown. Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 407 (2004); United States v. Microsoft Corp., 253 F.3d 34, 79 (D.C. Cir. 2001) (citation omitted) (the monopolist must be "engaged in anti-competitive conduct that reasonably appears to be a significant contribution to maintaining monopoly power."). This typically requires proof of exclusionary conduct to protect, create or enhance the monopoly that has an anti-competitive effect. *Grinnell,* 384 U.S. at 571 (distinguishing exclusionary conduct from competition on the merits); *Microsoft*, 253 F.3d at 58 (for conduct to be condemned as exclusionary, it must have an anti-competitive effect).

[21] Ford Motor Co. v. United States, 405 U.S. 562, 573 (1972) (citation omitted) (noting the court's "large discretion to fit the decree to the special needs of the individual case."); *Microsoft*, 253 F.3d at 105 ("[A] district court is afforded broad discretion to enter that relief it calculates will best remedy the conduct . . . .").

of fines or jail,[22] to injunctive or other equitable relief.[23] Damages are generally awarded only in private antitrust litigation, which offers plaintiffs the lure of treble damages.[24]

A well-designed antitrust remedy strives for three things: to achieve its objectives, to avoid unintended harm,[25] and to be administrable by the supervising court or agency.[26] In a government monopolization case, the objectives of an antitrust remedy are often described as ending the monopolist's unlawful conduct, preventing its recurrence and restoring "workable competition in the market."[27] In the broadest sense, though, the objective of an antitrust remedy is the same objective as antitrust law enforcement writ large—to improve consumer welfare through competition. As the Supreme Court explains, "Congress

---

[22] 15 U.S.C. § 2 (2018).

[23] 15 U.S.C. § 4 (2018) (empowering courts to grant equitable relief for violations of Sections 1–7 of the Sherman Act). *See also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (revised Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (table summarizing the remedial powers of the DOJ under the Sherman Act Sections 1 and 2).

[24] 15 U.S.C. § 15 (2018). Generally, only private plaintiffs can seek damages in antitrust suits, *but see* 15 U.S.C. § 15a (2018) (allowing suits by the U.S. for damages when injuries are sustained directly by the U.S. government). Damages are rare in government cases.

[25] Spencer Weber Waller, *The Past, Present, and Future of Monopolization Remedies*, 76 ANTITRUST L.J. 11, 12 (2009) ("[T]he merits of any chosen remedy should not be markedly outweighed by its costs or its harm to innocent parties and should be in the overall public interest.").

[26] Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 415 (2004) (quoting Phillip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 853 (1990)) ("No court should impose a duty to deal that it cannot . . . reasonably supervise."). Compensation of victims is often also articulated as a remedial objective of antitrust, but that objective largely relates to private litigation, not the government suits discussed here.

[27] United States v. United Shoe Mach. Corp., 391 U.S. 244, 251–52 (1968) (citation omitted) (stating that "principal objects" of district court's remedy are "to extirpate practices that have caused or may hereafter cause monopolization, and to restore workable competition in the market"); United States v. Microsoft Corp., 253 F.3d 34, 103 (D.C. Cir. 2001) (describing antitrust remedial goals as ending the anti-competitive conduct, ending the illegal monopoly, ensuring that there remain no practices likely to result in monopolization in the future and denying the defendant the fruits of its violation).

designed the Sherman Act as a consumer welfare prescription."[28] This means antitrust law seeks to promote competition in markets, as a means of achieving consumer welfare through higher output, better quality and lower prices for products and services.[29] Over the last 40 years, consumer welfare has been the yardstick for determining which mergers and unilateral conduct are prohibited by antitrust law.[30] Misconduct that reduces consumer welfare is condemned, while conduct that improves consumer welfare is permitted. Thus, a remedy that fails to improve consumer welfare, or even reduces it, undermines the very purpose of bringing an antitrust case.

The second goal of an effective remedy, avoidance of unintended harm, can also be framed as a corollary of the consumer welfare standard in antitrust law. A poorly designed antitrust remedy could cause more harm to consumers than the original misconduct.[31]

Many high-tech cases present a special challenge in this regard. As the wild animal analogies in the introduction of this article suggest, technology markets are often complex, dynamic and unpredictable in nature.[32] Remedies must not only grapple with effective intervention into such a market at the time of the case, but also look ahead at how to restore competition and prevent the recurrence of the misconduct. This crystal ball gazing is difficult in light of the sheer speed of change and

---

[28] Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979).

[29] Donald F. Turner, *The Durability, Relevance, and Future of American Antitrust Policy*, 75 CALIF. L. REV. 797, 798 (1987).

[30] *See, e.g.*, Christine S. Wilson, Commissioner, Fed. Trade Comm'n, Keynote Address, Welfare Standards Underlying Antitrust Enforcement: What You Measure Is What You Get, George Mason Law Review 22d 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.

[31] Barnett, *supra* note 2, at 32 ("[A] bad Section 2 remedy risks hurting consumers . . . and thus is worse than no remedy at all.").

[32] David Balto & Robert Pitofsky, *Antitrust and High-Tech Industries: The New Challenge*, 43 ANTITRUST BULLETIN 583, 584–86 (1998) (noting these characteristics make monopolization enforcement difficult in technology industries); DOJ SINGLE-FIRM CONDUCT GUIDELINES, *supra* note 1, at 158 (noting rapid change and innovation in new–economy industries raise "special challenges" for remedies).

substantial complexity of many technology markets. Software versions, products and even business models often become obsolete within a manner of months, but antitrust remedies last for decades. Balto and Pitofsky explain the risk this creates: "[a] remedy that is imposed on a technology that is rapidly being outmoded may do nothing to enhance consumer welfare, and may, in fact, impose costs on an industry that could lead to a reduction in innovation."[33] Since digital platforms are among the most innovative and dynamic companies in the world, it is essential to think carefully about those costs in designing monopolization remedies.[34]

The third goal, administrability of the remedy, is not just a matter of convenience for the courts—it goes to the fundamental willingness of the judiciary to grant a remedy. The Supreme Court has warned that in antitrust cases, "[n]o court should impose a duty to deal that it cannot explain or adequately and reasonably supervise."[35] If it appears that such a remedy is required, then antitrust law may not be suited to correcting the misconduct. Where remedies require the court to go as far as assuming day-to-day, regulatory-like supervision of the defendant, "[t]he problem should be deemed irremedia[ble] by antitrust law."[36] As discussed later in this article, these three remedial goals—achieving the enforcement objectives, avoiding unintended harm and ensuring administrability—can find themselves in tension when data access remedies try to accommodate consumer data privacy interests.

---

[33] Balto & Pitofsky, *supra* note 32; DOJ SINGLE-FIRM CONDUCT GUIDELINES, *supra* note 1, at 159 (observing that in dynamic industries, long term remedies may have "damaging, unintended consequences").

[34] Marina Lao, *No-Fault Digital Platform Monopolization*, 61 WM. & MARY L. REV. 755, 764 (2020) (in response to calls for drastic remedies against dominant digital platforms, observing that "it would be prudent to have some reliable evidence . . . that the economic benefits of dispersing the platforms' power outweigh the losses, before any attempt is made to restructure some of the country's most creative and successful companies.").

[35] Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 415 (2004).

[36] *Id.*

B. Introduction to Data Access Remedies and Digital Platform Monopolization Theories

Digital platforms have faced calls for nearly every type of remedy, from structural remedies that break up their businesses[37] or limit vertical integration,[38] to behavioral remedies that require neutral treatment of rivals using their digital services,[39] or a combination of these options.[40] Others call for remedies that are not antitrust law at all, such as public-utilities style regulation.[41]

---

[37] Khan, *supra* note 10, at 981 (2019) (arguing dominant technology platforms should be subject to structural separation, such as forcing Amazon to separate its "platform" of Amazon Marketplace from the remainder of its business); Warren, *supra* note 9 (proposing structural separation for large platforms).

[38] Khan, *supra* note 10, at 1024–25.

[39] *See, e.g., Hearing on Google's Use of Consumer Data Before H. Antitrust Subcomm.*, 115th Cong. (2018) (statement of Rep. David Cicilline, Member H. Antitrust Subcomm.), https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns&start=7645 (informing the CEO of Google he "plan[s] to work with the Federal Trade Commission to develop legislation" imposing non-discrimination obligations on digital platforms).

[40] Antitrust remedies are often discussed as either "structural" or "behavioral"/"conduct" remedies. *See, e.g.*, DOJ SINGLE-FIRM CONDUCT GUIDELINES, *supra* note 1, at 149 (discussing "structural" vs. "conduct" remedies). A structural remedy seeks to change the market or company through divestiture or dissolution into separate operating businesses. A behavioral remedy seeks to control the conduct of the defendant, by preventing or requiring certain action, or both. Though a convenient division for the purposes of discussion, structural and behavioral remedies are not mutually exclusive, and a blend of both may be imposed in a "belt and suspenders" approach. *Id.* at 150 ("Conduct and structural remedies need not be mutually exclusive. In some instances, relief with both conduct and structural aspects may be needed."); *see also* United States v. Am. Tel. & Tel. Co., 552 F. Supp. 131 (D.D.C. 1982). To the extent that cases against digital platforms end in a mix of both structural and data access remedies, the conduct element would raise many of the same data privacy issues discussed here.

[41] Ben Smith, *George Soros Just Launched a Scathing Attack on Google and Facebook*, BUZZFEED NEWS (Jan. 25, 2018), https://www.buzzfeednews.com/article/bensmith/george-soros-just-launched-a-scathing-attack-on-google-and (arguing "giant IT companies" are "near-monopoly distributors" that should be treated as public utilities).

But history tells us that a behavioral remedy is the most likely outcome in a Section 2 cases against digital platforms.[42] A structural remedy in a monopolization case "has rarely been sought or achieved in modern times outside of the AT&T breakup" in the early 1980's.[43] Less than 10% of non-merger cases brought by agencies through 1999 ended in structural remedies.[44] In fact, the FTC and EU authorities have already expressed skepticism in response to calls for structural remedies against digital platforms, with one FTC Commissioner calling structural orders a "last resort."[45]

This article focuses on growing calls for a specific type of behavioral remedy, one that grants access to or requires disclosure of data as a means of enabling online competition with digital platforms.[46] The term "data access" remedy is used

---

[42] William H. Page, *Mandatory Contracting Remedies in the American and European Microsoft Cases*, 75 ANTITRUST L.J. 787, 789 (2009) (explaining that history suggests structural remedies are unlikely in public monopolization cases and discussing failure of efforts to obtain a structural remedy against Microsoft); Noah Joshua Phillips, Commissioner, Fed. Trade Comm'n, We Need to Talk: Toward a Serious Conversation About Breakups, Hudson Institute, at 4–5 (Apr. 30, 2019), https://www.ftc.gov/system/files/documents/public_statements/1517972/phillis_-_we_need_to_talk_0519.pdf (clarifying the oft-stated preference for structural remedies refers to mergers, not monopolization cases) ("Where conduct triggers Section 2 liability, antitrust agencies and courts almost always seek behavioral remedies . . . .").

[43] Spencer Weber Waller, *Access and Information Remedies in High-Tech Antitrust*, 8 J. COMP. L. & ECON. 575, 577 (2012); *see also* United States v. Am. Tel. and Tel. Co., 552 F. Supp. 131 (D.D.C. 1982).

[44] Phillips, *supra* note 42, at 6; *see also* Robert W. Crandall, *The Failure of Structural Remedies in Sherman Act Monopolization Cases*, 80 OR. L. REV. 109, 116 (2001) (51.2% of civil cases through 1996 had behavioral remedies, 20.5% compulsory licensing, and 28.3% structural relief). Though presenting slightly different figures through 1996, this article similarly indicates that structural relief is significantly less common than behavioral remedies.

[45] Phillips, *supra* note 42, at 20; *see also* Stephanie Bodoni & Aoife White, *Breaking Up Tech Giants Would Be Hard to Do, EU's Vestager Says*, BLOOMBERG LAW, Jan. 25, 2019.

[46] Hoffman, *supra* note 13, at 13 ("[D]oes antitrust provide an answer to whatever problems may exist with the accumulation of data? Some commentators at the hearing thought the answer lay in utility-style regulation - requiring firms to share their data troves."); Vestager, *supra* note 13 ("[O]ne thing we may need to do, to open up competition, is to require companies to give rivals access to their data.").

here to refer to a behavioral remedy in which a court order, issued in either in a litigated case or as part of a consent agreement, requires the defendant to provide access to information it holds. In keeping with the goals of antitrust remedies described above, the purpose of granting such access would be to restore competition, based on the premise that data access is necessary to compete.[47]

The mechanism for providing a data access remedy could be simply a requirement to disclose the information, or, more likely, an obligation to interoperate with rivals or treat rivals neutrally to the company's own vertically-integrated products or services.[48] Access, interoperability and neutrality obligations may be quite distinct in other contexts, but for digital platforms like social media or search, the three concepts are often related or overlapping. Though somewhat simplified, for digital platforms these remedies may share the purpose of providing a rival with access to user data: access through interoperability,[49] access through neutrality obligations,[50] or simply direct data access through disclosure.

---

[47] *See* discussion *infra* Section III.A.1. *Digital Platform Monopolization Theories and Remedies Implicate Consumer Data*.

[48] *See, e.g.*, WILSON C. FREEMAN & JAY B. SYKES, ANTITRUST AND "BIG TECH" 35 (2019) (contemplating "interoperability" standards that require companies to "minimize technical impediments to the use of complementary products").

[49] Take, for example, the recent Ninth Circuit case *hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019)*. Upstart hiQ competes with LinkedIn to sell software that analyzes LinkedIn user profile data. The software is sold to employers and recruiters who want to be alerted when LinkedIn users update their profile, an indication they may be about to switch jobs. HiQ obtained an interim order securing its interoperability with LinkedIn's social networking service, based on unfair competition law and other claims. HiQ did not seek interoperability for the sake of somehow simply being "on" or connected with LinkedIn's service. Rather, hiQ wanted interoperability to gain access to user profile data hosted by LinkedIn, which hiQ then uses for its data analytics software.

[50] Neutral treatment by a digital platform may be sought for the purpose of reaching consumer data through that platform. For example, vertical search engines obtain data from consumers when they appear as links within Google's general search results, and consumers click through to their website. Some theorize that neutral treatment by Google in how it ranks search results may enable competition because it increases the search data

The discussion of access remedies in U.S. law often begins with the observation that antitrust courts are skeptical of enforced sharing of competitive resources.[51] The primary concern is that requiring firms to share the source of their competitive advantage will lessen the incentives of both the monopolist and its rivals to invest in such facilities, and in doing so, reduce the facilities-based competition that antitrust law seeks to promote.[52] Such remedies also raise administrability concerns, in particular, the institutional competency of courts to oversee ongoing resource sharing, a task which may be more regulatory than judicial in nature.[53]

However, these concerns have not stopped data access remedies from playing a prominent role in settlement agreements.[54] This is particularly true in antitrust litigation

---

these vertical search engines are able to collect from consumers, which they use to improve their algorithms and search results. Neutral treatment could be achieved by the platform either granting rivals access to data or a facility, or by blocking both the platform and the rival from access. Denial of access to data means consumers lose out on any data-driven benefits, such as product or service design improvements. Merger remedies have used the approach of denying access to data, *see e.g.* Competitive Impact Statement at 13–14, United States v. Google Inc., No. 1:11-cv-00688 (D.D.C. Apr. 8, 2011), www.justice.gov/atr/cases/f269600/269620.pdf (describing the merger remedy requirement of a firewall to prevent Google from using ITA data).

[51] *See e.g.* Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 408 (2004).

[52] *Id*. at 407–08. Classic essential facilities cases have involved the question of whether to grant access to a competitor's physical facilities. *See e.g. id*. (rival seeking access to telephone network); Aspen Highlands Skiing Corp. v. Aspen Skiing Co., 738 F.2d 1509, 1519 (10th Cir. 1984), aff'd, 472 U.S. 585 (1985) (seeking access to ski resorts); MCI Communications Corp. v. American Telephone & Telegraph Co. 708 F.2d 1081 (7th Cir. 1983) (seeking interconnection access to local telephone circuits); Otter Tail Power Co. v. United States, 410 U.S. 366 (1973) (involving access to electric power transmission facilities).

[53] Verizon Commc'ns Inc., 540 U.S. at 408 ("Enforced sharing also requires antitrust courts to act as central planners, identifying the proper price, quantity, and other terms of dealing–a role for which they are ill suited.")

[54] *See* e.g. *infra* Section III.A. *Past Monopolization Remedies Ordered Disclosure of Company Information: The Computing Cases* (discussing settlement agreements in computing industry cases that imposed data access obligations).

involving network industries, software platforms, and other high technology sectors.[55] The businesses of digital platforms share all of these characteristics. As the economic value of information grows, so too has emphasis on this type of disclosure-focused antitrust remedy.[56] Data access remedies may be more likely in digital platform cases than indicated by the baseline position of judicial skepticism.

Increasingly, data access remedies have become part of the conversation on digital antitrust enforcement. The head of the European Union's competition authority warned imminently that "as data becomes increasingly important for competition, it may not be long before the Commission [the EU-level antitrust authority] has to tackle cases where giving access to data is the best way to restore competition."[57] Reports to antitrust authorities in the U.K. and the EU have recommended forced data sharing by large online companies to promote effective competition in digital markets.[58]

In the U.S., the FTC's recent hearings on privacy, data and competition in the 21st century devoted a panel to remedies, and considered compulsory data access.[59] Data access remedies are also tacitly being invoked by those who hold up *United States v. Microsoft Corp.* ("*Microsoft*") as a model for the revival of anti-monopolization enforcement.[60] This seminal technology monopolization case ended in a 2002 settlement agreement that required Microsoft to provide data access to its

---

[55] Waller, *supra* note 43, at 576.

[56] *Id*. at 575 ("In an economy increasingly dominated by information and information technology, it is not surprising that antitrust remedies increasingly also have focused on the disclosure of competitively necessary information . . . .").

[57] Vestager, *supra* note 13.

[58] U.K. COMPETITION EXPERT PANEL, UNLOCKING DIGITAL COMPETITION: REPORT OF THE DIGITAL COMP. EXPERT PANEL ¶ 2.81 (Mar. 2019) ("[I]n some markets, the key to effective competition may be to grant potential competitors access to privately-held data.").

[59] FED. TRADE COMM'N, *Hearings on Competition and Consumer Protection in the 21st Century, Hearing No. 6: Privacy, Big Data, and Competition*, American University Washington College of Law, Hr'g Tr. 73, Remedies for Competition Problems in Data Markets (Nov. 2018).

[60] 253 F.3d 34 (D.C. Cir. 2001) (en banc).

rivals.[61] Further, in recent private antitrust litigation, rivals obtained interim data access from the social media platforms Twitter and LinkedIn.[62] The potential for a data access remedy looms large in impending cases against digital platforms, notwithstanding the general skepticism of U.S. courts toward such remedies.

Data access remedies have entered the conversation on digital platforms in no small part because of new theories of monopolization focused on data accumulation. For example, Maurice E. Stucke and Allen P. Grunes argue that data itself is the source of monopoly power of digital giants, labelling the vast stores of data held by digital platforms "data-opolies."[63] They contend that data-opolies, like monopolies, confer competitive advantages that are being used to exclude rivals from access to information necessary to compete.[64] Howard A. Shelanski and others similarly argue that the massive accumulation of data by incumbent monopolists is a "strategic asset" that acts as a barrier to entry, foreclosing competition.[65]

---

[61] United States v. Microsoft, No. 98-1232 (CKK), 2009 WL 1348218, at *6 (D.D.C. Apr. 22, 2009) (originally entered Nov. 12, 2002; modified Sept. 7, 2006; further modified Apr.22, 2009); United States. v. Microsoft Corp., 231 F. Supp. 2d 144 (D.D.C. 2002), *aff'd sub nom.* Massachussets v. Microsoft Corp., 373 F.3d 1199 (D.C. Cir. 2004) (resulting in approval of consent decree).

[62] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (granting a temporary injunction to prevent LinkedIn from terminating hiQ's access to the LinkedIn social networking service); PeopleBrowsr, Inc. v. Twitter, Inc., No. C–12–6120 EMC, 2013 WL 843032, at *1 (N.D. Cal. Mar. 6, 2013) (granting a temporary injunction to prevent Twitter from terminating PeopleBrowsr's access to Twitter's feed of users' social media posts).

[63] ALLEN P. GRUNES & MAURICE STUCKE, BIG DATA AND COMPETITION POLICY 277 (2016).

[64] *Id.*; Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimize Quality: A Look at Search Engines*, 18 YALE J.L. & TECH. 70, 103 (2016); Eur. Data Prot. Supervisor, Privacy and Competitiveness in the Age of Big Data 30–31 (2014) (describing a line of 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 from competitors").

[65] Howard A. Shelanski*, Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1679 (2013); *see also*, Damien Geradin & Monika Kuschewsky, *Competition Law and Personal*

These theories treat data akin to an essential facility to which rivals require access to compete. This casting of data as essential to competition, in turn, prompts calls for data access remedies. The newer theories of competitive harm center around accumulation of and denial of access to data, and therefore the related remedies discussion turns to providing rivals with access to that data. The more data-centric monopolization theories take root, the greater the specter of data access remedies.

These data monopolization theories are new and divisive. Opposing scholars are skeptical that data can confer a monopoly at all, given its non-rivalrous nature.[66] Even when data is accumulated in large amounts, they argue the competitive importance of data-related network effects and scale advantages as barriers to entry are exaggerated for digital platforms.[67] Other

---

Data: Preliminary Thoughts on a Complex Issue, 2 CONCURRENCES 2 (2013) ("The acquisition of large volumes of data by 'first mover' providers may, however, raise barriers to entry and thus deprive users from the benefits of competition."); 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, 775 n.18 (2010) ("[T]he need to amass huge troves of data, or one firm's huge lead in assembling such a data trove, might be characterized an entry barrier."); Nathan Newman, *Search, Antitrust and the Economics of the Control of User Data*, 31 YALE J. REG. 401 (2014).

[66] Anja Lambrecht & Catherine E. Tucker, *Can Big Data Protect a Firm from Competition?*, CPI ANTITRUST CHRON., Jan. 2017, at 5–6 (arguing data is non-rivalrous, meaning more than one entity can hold the same data, and data is available from multiple different sources, therefore it is unlikely to act as a sustainable barrier to competition); Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, 14 ANTITRUST SOURCE, Dec. 2014, at 3 (arguing data is non-rivalrous and non-exclusive, meaning the same data can be collected and used by multiple firms); D. Daniel Sokol and Roisin E. 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, where entry can occur based on an innovative new product that is used as a springboard to quickly collect additional user data).

[67] Sokol & Comerford, *id.* at 1135 ("[T]he unique economic characteristics of data mean that its accumulation does not, by itself, create a barrier to entry, and does not automatically endow a firm with either the incentive or the ability to foreclose rivals, expand or sustain its own monopoly, or harm competition in other ways."); Catherine Tucker, *Network Effects and Market Power: What Have We Learned in the Last Decade?*, 32 ANTITRUST L.J. 72, 72 (2018) ("[O]ur understanding of network effects has evolved in the digital economy. These new findings

factors, such as engineering talent or product design, may more often explain the success of digital businesses.[68]

These liability-stage disagreements are debated at length in other articles.[69] Instead of focusing on the liability debate, this article seeks to bring new perspective to digital antitrust theories by looking ahead to remedies. Though rooted in skepticism of data monopolization theories, this article accepts their premise for the purpose of discussing what would occur if those theories formed the basis of a Sherman Act Section 2 violation. This thought exercise highlights as-yet unacknowledged tensions between data privacy and data access remedies.

The potential for tension between antitrust data access remedies and data privacy is clear, yet has seen little analysis to date. As this article explains, data access remedies against digital platform monopolists may well require access to consumers' private information.[70] While FTC data privacy enforcement works to limit the collection, use and sale of consumer information online, a data access remedy could do the opposite,

---

suggest that network effects are not the guarantor of market dominance that antitrust analysts had initially feared."); 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."); Andres V. Lerner, *The Role of "Big Data" in Online Platform Competition* (Aug. 26, 2014), http://ssrn.com/abstract=2482780 (arguing there are alternative means to acquire data and scale necessary for new entrants to compete).

[68] Lambrecht & Tucker, *supra* note 66, at 8 (providing the examples of online dating app Tinder or home rental service Airbnb as data-poor upstarts whose superior customer solutions and user interfaces led to massive popularity over incumbents with more data).

[69] *See, e.g.*, sources cited *supra* note 65-67; Herbert J. Hovenkamp, *Whatever Did Happen to the Antitrust Movement?,* 94 NOTRE DAME L. REV. 583; Lao, *supra* note 34 (discussing theories of no-fault digital monopolization).

[70] *See infra* Section III.A.1. *Digital Platform Monopolization Theories and Remedies Implicate Consumer Data*.

requiring that rivals be permitted to access and use consumers' private information.[71]

II. EXISTING THEORIES ON THE INTERSECTION OF ANTITRUST LAW AND DATA PRIVACY

Theories of interaction between competition, antitrust law and data privacy are only beginning to develop. This is unsurprising given the newness of data privacy law. Data privacy protection and anti-monopolization enforcement have only recently begun to coexist in U.S. law. Over the last 25 years, the Federal Trade Commission has established "the new common law of privacy," and become the *de facto* U.S. regulator of the use and collection of consumer data.[72] This rise of data privacy law coincides precisely with a period of near-absent monopolization enforcement by antitrust agencies.[73] As Tim Wu explains, "[i]n the United States, there have been no trustbusting or 'big cases' for nearly twenty years."[74] *Microsoft* is often held up as the last major Section 2 Sherman Act case, but the bulk of that dispute ended with a settlement agreement in 2002.[75] Private parties continue to bring civil anti-monopoly litigation, but these cases lack the power and significance of agency cases, and certainly do not threaten the same likelihood of success. Around the time data privacy started to take hold in the U.S., "the anti-monopoly provisions of the Sherman Act went into a deep freeze from which they have never really recovered."[76] Now that monopolization enforcement is unthawing, these areas of law are poised to interact in new and complex ways.

---

[71] *See infra* Section III.B.1. *The Rise of Data Privacy Law and its Application to Digital Platforms*.

[72] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–600 (2014).

[73] WU, *supra* note 10, at 108.

[74] *Id.* at 110.

[75] United States v. Microsoft, No. 98-1232 (CKK), 2009 WL 1348218, at *6 (D.D.C. Apr. 22, 2009) (originally entered Nov. 12, 2002; modified Sept. 7, 2006; further modified Apr. 22, 2009).The Bush Administration's DOJ brought no new anti-monopoly cases. There were blips of increased enforcement during the Clinton and Obama years, but no groundbreaking Section 2 cases on the scale of *Microsoft*, 253 F.3d 34.

[76] WU, *supra* note 10, at 108.

How, then, does antitrust law interact with data privacy protection? As this section explains, there are two main theories in the literature on this interface. The first considers data privacy to be entirely outside the ambit of antitrust law. The second integrates data privacy into antitrust analysis as an element of quality-based competition. However, both theories focus on the liability stage of antitrust analysis. They stop short of addressing the potential impact of data privacy on antitrust remedies. Application of this liability-stage thinking can miss the consumer data privacy impacts that arise from antitrust remedies.

A. The Separatists: Data Privacy is Beyond the Purview of Antitrust Law

The first school of thought on the antitrust/data privacy interface posits that there is no such interface at all. It insists that data privacy is beyond the purview of antitrust law.[77] This view is labelled "separatist" theory here, because its proponents emphasize the historical and doctrinal separation between antitrust law and data privacy law. The leading paper on this topic, written by Ohlhausen and Okuliar, traces the doctrinal distinction between antitrust law and data privacy law throughout the institutional history of the FTC.[78] Initially, the FTC had only the power to bring competition cases. Later, the agency was granted statutory consumer protection powers to address unfair and deceptive practices,[79] which the FTC grew into the *de facto* data privacy law of the U.S. today. This separation persists in the branches of legal doctrine on data

[77] *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 "antitrust is the wrong vehicle to address privacy concerns"); Allen P. Grunes, *Another Look at Privacy*, 20 GEO. MASON L. REV. 1107, 1113–14 (2013) (summarizing the position in literature that "rare" privacy harms "seem better dealt with by privacy laws or adverse publicity than by antitrust litigation"); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right *[Approach]* to Privacy, 80 ANTITRUST L.J. 121, 138–43 (2015).

[78] Ohlhausen & Okuliar, *supra* note 77.

[79] 15 U.S.C. § 45(a)(1) (2018), enacted by H.R. REP. NO. 751613, at 3 (1937).

privacy and competition, and even in the institutional design of the FTC.[80]

Ohlhausen and Okuliar argue that the legal analysis of data privacy and antitrust law ought to remain separate, because each area of law seeks to protect against different harms. Antitrust law, they claim, is better suited to addressing conduct harmful to overall consumer welfare or economic efficiency. Meanwhile, data privacy law is better suited to ensuring that individual consumers receive the benefit of their bargain, given its focus on informed choice and reasonable consumer expectations.[81] Ohlhausen and Okuliar's article, and other similar literature, endeavors to categorize misconduct into that best addressed by antitrust law and that best addressed by data privacy law, based on these perceived differences.[82] In their view, neither of these areas of law would, or should, address the same misconduct.

B. The Integrationists: Data Privacy Is an Element of Product Quality

The other main view on this intersection theorizes that antitrust law ought to consider data privacy when it is an element of non-price competition.[83] This theory integrates data privacy

---

[80] The FTC's Bureau of Consumer Protection has jurisdiction over data privacy and data security cases, while the FTC's Bureau of Competition has jurisdiction over certain antitrust cases, along with the Department of Justice Antitrust Division.

[81] Ohlhausen & Okuliar, *supra* note 77, at 154–55.

[82] *Id.* (distinguishing between conduct that ought to be addressed by consumer protection law and antitrust law); *see also* Eugene Kimmelman, et al., *The Limits of Antitrust in Privacy Protection*, 8 INT'L DATA PRIVACY L. 270 (2018) (distinguishing between privacy harms best addressed by consumer protection law frameworks and anti–competitive conduct related to data); Sokol & Comerford, *supra* note 66, at 1133, 1156–58 ("[T]he distinct issues addressed by antitrust and consumer protection law . . . are distinct for good reason, and are complements, rather than substitutes.").

[83] Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis ("[P]rivacy harms can lead to a reduction in the quality of a good or service. . . . Where these sorts of harms exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them."); *see also* Allen P. Grunes &

into existing antitrust conceptions of consumer welfare, and so is referred to here as "integrationist" theory. Integrationists reject the separatist view as an "artificial dichotomy" that "makes no sense to maintain," given that both areas of law seek to promote consumer welfare.[84] Integrationist theory is the most developed conception of how antitrust and data privacy intersect,[85] and has garnered more acceptance from scholars and agencies than any other view. The FTC,[86] DOJ[87] and European competition authorities[88] have adopted this integrated view in

---

Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, ANTITRUST SOURCE, May 2015, at 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."); Harbour & Koslov *supra* note 65, at 773 ("[P]rivacy is an increasingly important dimension of competition as well, which is exactly why modern antitrust analysis must take privacy into account.").

[84] Julie Brill, *The Intersection of Consumer Protection and Competition in the New World of Privacy*, 7 COMPETITION POL'Y INT'L 7, 8–10 (2011); Harbour & Koslov *supra* note 65, at 773.

[85] Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON., May 2014, at 2–3, 4–5 (disagreeing with the approach of considering privacy as an element of quality, but noting it is one of the most developed theories).

[86] Deborah Feinstein, *Big Data in a Competition Environment*, CPI ANTITRUST CHRON., May 2015, at 2 ("[T]he FTC has explicitly recognized that privacy can be a non-price dimension of competition."); Fed. Trade Comm'n, *Statement of FTC Concerning Google/DoubleClick*, FTC File No. 071-0170, 2–3 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf; Noah Joshua Phillips, Commissioner, Fed. Trade Comm'n, Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy, The Center for Internet and Society, Stanford Law School, at 3 (Jan. 30, 2020), https://www.ftc.gov/system/files/documents/public_statements/1565039/phillips_-_stanford_speech_10-30-20.pdf ("Privacy can be evaluated as a qualitative parameter of competition, like any number of non-price dimensions of output . . . .").

[87] Makan Delrahim, Assistant Attorney General, Dep't of Justice, "…And Justice for All": Antitrust Enforcement and Digital Gatekeepers, Speech at Antitrust New Frontiers Conference in Tel Aviv, Israel (June 11, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers ("[D]iminished quality is also a type of harm to competition. . . . [P]rivacy can be an important dimension of quality.").

[88] Margrethe Vestager, Comm'r of Competition, Eur. Comm., Mackenzie Stuart Lecture at Cambridge: Making the Data Revolution Work

theory and in their analysis, though privacy-based competition has not been determinative in any U.S. cases.

The integrated view begins from the well-established position in antitrust law that price is not the only basis for competition. As the Supreme Court explains, "all 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."[89] Antitrust law seeks to improve consumer welfare through competition, and such competition can occur in markets based on many factors other than price, including product quality, variety, and innovation. From there, the integrationist view simply takes a broad perspective on what constitutes "quality," incorporating competition based on data privacy as a sub-type of quality competition. In other words, for some products and services "[c]ompanies compete to offer more or less privacy to users."[90] When data privacy is an element of such quality-based competition, integrationist theory dictates that antitrust law take privacy into account.

Integrationist theory originated with, and tends to focus on, merger review.[91] It posits that if the merging firms compete

---

for Us (Feb. 4, 2019) ("[I]f privacy is something that's important to consumers, competition should drive companies to offer better protection."); *see, e.g.*, Eur. Comm'n, Facebook/WhatsApp, Case No. COMP/M.7217 C(2014) 7239, ¶ 174 (Mar. 10, 2014) [hereinafter Facebook/WhatsApp EU Decision] (acknowledging privacy as a non-price element of competition); European Commission Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 (same).

[89] Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 695 (1978).

[90] Pasquale, *supra* note 4, at 1009.

[91] Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007, 9:00 AM), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis (noting "[t]here was little or no analysis of the intersection of antitrust and privacy before the announcement of the proposed merger of Google and DoubleClick" in 2007, and discussing privacy as quality in the merger context). For additional sources discussing data privacy and antitrust in mergers, see *supra* note 86.

with each other to offer more privacy protective products or services to consumers, the combination of those firms could reduce competitive pressure that drives each company to offer consumers new and better privacy features. The merger could thus lead to an erosion of data privacy as an element of product quality, harming consumers who prefer a higher level of data privacy protection. This type of argument was considered when Facebook sought to acquire WhatsApp, though U.S. and EU antitrust agencies concluded that such anti-competitive privacy impacts were unlikely to occur.[92]

Though less commonly discussed, similar arguments have been made regarding monopolization and data privacy. Harbour and Koslov argue, for example, that in Section 2 Sherman Act analysis, agencies should consider whether reduced competitive pressure to offer data privacy protection could cause a dominant firm to invest fewer resources in such

[92] Facebook/WhatsApp EU Decision, *supra* note 88; Alexei Oreskovic, *Facebook Says WhatsApp Deal Cleared by FTC*, REUTERS, Apr. 10, 2014; Though the transaction was not challenged by U.S. antitrust authorities, the FTC's data privacy law enforcement branch sent a letter warning that post-acquisition, WhatsApp must continue to honor its privacy promises to consumers, or risk Section 5 FTC Act privacy enforcement. *See* Letter from Jessica L. Rich, Office of the Dir. Bureau of Consumer Prot., Fed. Trade of Comm'n, to Erin Egan, Chief Privacy Officer, Facebook, Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.; *but see* Press Release, Fed. Trade Comm'n, FTC to Examine Past Acquisitions by Large Technology Companies (Feb. 11, 2020), https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies (announcing that FTC is re-opening its review of several closed mergers in the digital sector, including Facebook/WhatsApp). Samson Y. Esayas, *Privacy-As-A-Quality Parameter of Competition*, *in* COMPETITION LAW FOR THE DIGITAL ECONOMY, 156–57 (Bjorn Lundqvist & Michal S. Gal, eds., 2019) (canvassing arguments on data privacy based competition in the Facebook/WhatsApp merger). The companies both offered online messaging services, but WhatsApp provided consumers with higher levels of privacy protection. WhatsApp collected and used less private data, did not target ads using consumer data, and offered privacy features such as encrypted messaging to prevent interception of user communications. It was argued by opponents to the merger that the transaction would reduce competitive pressure on the merging parties to offer privacy protection to consumers in messaging services, harming consumers who prefer a more privacy-protective messaging service. *Id*.

privacy features for consumers. Privacy protection often has costs for the monopolist, both financial and the opportunity cost of the foregone uses of consumer data. These authors theorize that, in the face of weakened or eliminated privacy-based competition, a dominant firm might rationally choose not to offer consumers as much privacy protection.[93]

At its core, the difference between the separatist and integrationist views lies in how broadly each conceives of the consumer welfare standard. Both accept that the goal of antitrust law enforcement is to improve consumer welfare, but separatists conceive of "consumer welfare" more narrowly than integrationists, who include privacy as part of quality-based competition in assessing such welfare.

This difference reflects a microcosm of the broader debate in antitrust law over the scope of the consumer welfare standard. Consumer welfare has long been the organizing principle in antitrust law. Separatists see the consumer welfare standard as bringing discipline and predictability to previously scattered antitrust legal doctrine.[94] Their central concern is that expanding the consumer welfare standard to encompass other interests, such as privacy, will cause antitrust doctrine to lose this coherency, and thus its legitimacy. Ohlhausen and Okuliar explain:

> A[n] ... approach to antitrust that encompasses normative privacy concerns also would provide cover for the injection of other noncompetition factors into the analysis. As a normative matter, privacy is conceptually unsettled and, depending on who you ask, could include other rights, like property rights or human dignity. The introduction of these factors could shift antitrust law's focus away from efficiency and alter its

[93] Harbour & Koslov *supra* note 65, at 795.

[94] Cooper, *supra* note 77 at 1138, 1143 (arguing privacy should not be incorporated into antitrust analysis because doing so "would inject a large degree of additional subjectivity into antitrust analysis"); Ohlhausen & Okuliar*, supra* note 77, at 153.

relatively predictable and transparent application.[95]

C. Existing Theories on the Antitrust Law/Data Privacy Interface Do Not Address Remedies

The separatist and integrationist theories both stop short of considering specifically how antitrust remedies might impact data privacy. This is not a criticism, but rather a recognition that the intersection between antitrust law and data privacy is newly emergent. The interaction between these areas of law has additional touchpoints that have not yet been discussed or analyzed. There is not only a potential interface between data privacy and antitrust liability theory, but also with antitrust remedies. Antitrust remedies have been called a "neglected"[96] and "under-theorized area of antitrust law."[97] These observations ring true at the intersection of remedies with data privacy.

Unsurprisingly, the existing liability-stage theories cannot simply be exported to analyze remedies. Here, as in other areas of law, the liability analysis and the remedies analysis may raise distinct considerations.

Consider a hypothetical that illustrates the distinct privacy implications that could arise at the liability stage and remedies stage analysis of a digital platform case. Gmail is Google's popular online email service. Third-party applications often interoperate with Gmail to offer users additional features,

---

[95] Ohlhausen & Okuliar, *supra* note 77, at 153 (footnotes omitted).

[96] DOJ SINGLE-FIRM CONDUCT GUIDELINES, *supra* note 1, at 143 ("Notwithstanding their importance, the study of remedies has been somewhat neglected.").

[97] Keith N. Hylton, *Remedies, Antitrust Law, and Microsoft: Comment on Shapiro*, 75 ANTITRUST L.J. 773, 773–74 (2009) (observing the lack of scholarly examination of antitrust remedies and inapplicability of more general remedies literature to the context of antitrust law); *see also* Spencer Weber Waller, *The Past, Present, and Future of Monopolization Remedies*, 76 ANTITRUST L.J. 11, 11 (2009) ("A well-understood theory of remedies in monopolization and abuse of dominance cases does not exist at present in either the case law or the academic literature and may not even be possible.").

such as email organization, tone checking or auto-fill for message composition. Consumers download these applications.

Then, the apps use application programming interfaces ("APIs"), provided by Google, to interconnect with the consumers' Gmail accounts.[98] The applications earn their profit by using the data within consumers' emails to sell targeted behavioral advertising to advertisers, or for other products.[99] This business model enables the app's email features to be offered for free to consumers. Assume that in this hypothetical, Google earns a small share of the profit from each ad delivered by these applications via Gmail, creating the type of prior profitable relationship required for a refusal to deal claim in antitrust law.

Imagine Google then changes its policy and API permissions to block any non-Google applications that sell email advertising in Gmail. Since both Google and the apps sell online advertising, they are competitors. The policy change thus denies rivals of Google access to the data they were previously using to compete against the company. Despite the advice of brilliant antitrust lawyers, internal documents show that Google refused to deal with these rival applications because it sought to prevent competition with Google's own in-email ad sales. Assume Google's termination of access also reduced overall competition for in-mail advertising, driving up ad prices. The blocking of

[98] APIs enable software connections to platform services. In technical terms, an API makes available routines or protocols that perform common functions required to interface between third-party applications and the platform. APIs make it easier to develop interfacing applications or other software. United States v. Microsoft Corp., 253 F.3d 34, 53 (D.C. Cir. 2001). Third-party software developers regularly use APIs to create applications that interface with the services of platforms, such as Google's Gmail or Facebook's titular website.

[99] There are many such applications in reality. For example, the FTC recently brought a data privacy case against Unroll.me, which offered users a Gmail app for organizing email inboxes and unsubscribing from marketing emails. Instead of ads, Unroll.me earned its profit by searching user emails for purchase receipts, and selling market research to companies based on that information. Complaint, In re Unrollme, Inc., No. C-4692 (Dec. 16, 2019), https://www.ftc.gov/system/files/documents/cases/c-4692_172_3139_-_unrollme_complaint.pdf.

these apps also means Gmail users can no longer access the useful features, like auto-fill, that the third-party applications provided to consumers.

The DOJ brings a successful case, proving that Google violated Section 2 of the Sherman Act by excluding rival applications from access to users' email. Or, more likely, the case ends in a negotiated settlement agreement. The remedy includes data access. To restore competition, the remedy requires Google to reinstate the third-party applications' access to the contents of users' Gmail messages and to provide access to similar rival applications.

Assuming users have a privacy interest in their email contents, then this remedy reduces user data privacy. The remedy grants third-party applications access to the private Gmail messages of users, without their consent. In the absence of the remedy, this access would not have occurred. The impact on consumers looks much the same as other unauthorized access and use of their personal email contents,[100] and much like the conduct the FTC pursues against digital platforms as violations of consumer expectations of privacy.[101] The distinction from an FTC data privacy case is that this data access is mandated by the antitrust remedial order.

Consider how each of the existing theories on antitrust law and data privacy would analyze this hypothetical. The separatist view would ignore any data privacy impact, deeming it outside the scope of antitrust law. The integrationist view would look for privacy-related quality competition between Google and the rival applications, but would find none. Google and the apps were competing to sell online advertising, not competing to offer users improved email data privacy. The integrationist view calls for antitrust law to account for data privacy only where there is privacy as quality competition at stake, which is not the case here. In fact, it is the opposite; the

[100] This hypothetical sets aside for the moment questions of notice and consent, which are addressed at length later in this article. *See infra* Section IV.A.1. *Short-Term Reconciliation: Consent-to-Remedy*.

[101] *See* discussion of FTC enforcement of data privacy law pursuant to Section 5 of the FTC Act, *infra* Section III.B.1. *The Rise of Data Privacy Law and its Application to Digital Platforms*.

companies are competing to convince users to give up their email privacy for the purposes of ad targeting. Whichever company obtains the most extensive access to users' private email contents can offer the most granular criteria for ad targeting, and charge the most to advertisers for that targeting ability. Neither theory would consider whether the data sharing remedy imposed here might impair user privacy. Nor should the theories be expected to; the legal analysis at the liability stage and remedies stage is distinct in many areas of law.

This example shows that even if a monopolist's misconduct is not "about" data privacy competition, the remedy itself could impact data privacy. Google's antitrust misconduct was, in fact, privacy-promoting. It reduced third-party access to users' email contents. It was the intervention of antitrust law with a data access remedy that reversed the user privacy protection offered by Google through its policy change. Existing theories on the intersection of data privacy and antitrust law do not address this remedies-stage tension.

III. CONTRASTING HISTORICAL AND CONTEMPORARY DATA ACCESS REMEDIES AGAINST PLATFORMS

This section considers monopolization cases that ended in data access remedies. In particular, it looks at cases against software and telephone directory monopolists who, like the digital giants of today, operated dominant, two-sided platform businesses characterized by network effects. The selected cases also involve allegations of exclusionary conduct, much like the theories against digital platform today.

The difference, however, is that none of these older cases had cause to consider consumer data privacy. This is because historical data access remedies tended to involve disclosure of company information, not consumer data. The nature of the information meant there was no reason to consider impacts on consumer data privacy. The rare monopolization cases that did order disclosure of private consumer information pre-date the rise of U.S. data privacy law. The new calls for data access remedies against digital platforms thus raise unprecedented

questions of whether and how to account for consumer data privacy in the design of data access remedies.

A. Past Monopolization Remedies Ordered Disclosure of Company Information: The Computing Cases

Many technology giants of the past have faced monopolization cases that ended in data access remedies. This section considers the disclosure obligations in three such cases: *Microsoft*, *In the Matter of Intel Corporation* ("*Intel*") and *United States v. International Business Machines Corporations* ("*IBM*") (together, the "computing cases").

At the time of their respective cases, each of these companies held market power, with a market share of 85% or more.[102] They were the "big tech" of old, reminiscent in market position to the digital platforms of today. Each company used its respective market power to engage in anti-competitive conduct that excluded new competitors.[103]

---

[102] *Microsoft*, 253 F.3d at 54–56 (Microsoft held 95% of worldwide sales in the market for "Intel-compatible PC operating systems"; concurring with District Court finding "in its entirety" that Microsoft had market power in the relevant market). Though market share is not enough, standing alone, to prove market power, it is often influential. The operating system market in *Microsoft* was characterized by strong network effects and barriers to entry that contributed to the finding of market power. *Id.*; Complaint at ¶ 3, Intel Corp., 150 F.T.C. 420 (2010) [hereinafter, *Intel Complaint*] ("Intel holds monopoly power in the markets for personal computer and server CPUs, and has maintained a 75 to 85 percent unit share of these markets since 1999."); Charles F. Phillips, Jr., *The Consent Decree in Antitrust Enforcement*, 18 WASH. & LEE L. REV. 39, 52 (1961) (explaining that IBM owned more than 90 percent of all tabulating machines, the computing technology at issue in the case, and sold over 90 percent of the cards used in the machines in the U.S.).

[103] The *Microsoft* and *IBM* cases involved Sherman Act Sections 1 and 2 violations. Intel was instead accused of violating the competition provisions of Section 5 of the FTC Act, but this difference was because the FTC brought the case against Intel, rather than the DOJ. The FTC does not have Section 2 Sherman Act enforcement power. Section 5 of the FTC Act covers similar conduct to Section 2 and, some argue, even more. The theories of harm against Intel focused on monopolization and attempted monopolization, and could just as easily have been the basis for a Sherman Act claim if brought by the DOJ or a private plaintiff. In fact, private claims

Microsoft sought to block emerging competition from Internet browsers. Browsers threatened to disintermediate the dominant Microsoft Windows operating system as the means by which computer users accessed software.[104] To end this threat, Microsoft engaged in a long list of anti-competitive conduct.[105] IBM used restrictive leasing practices to squeeze out competitors that manufactured or maintained tabulating card or "punch card" computing systems. Intel refused to deal with rival makers of graphics processing units ("GPUs"), a product that initially interoperated with, but eventually threatened to replace, Intel's central processing units ("CPUs") for computers.[106] Intel was accused of withholding interoperability information about pending CPU models, and even of providing inaccurate information about Intel product interfaces, which caused its GPU rivals to lose time and money designing products that

---

were pursued under Section 2 Sherman Act for similar misconduct by Intel in Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1291 (N.D. Ala. 1998), *rev'd on other grounds*, 195 F.3d 1346 (Fed. Cir. 1999).

[104] *Microsoft*, 253 F.3d at 59–60. The then-new phenomenon of internet browsers, particularly Netscape Navigator, threatened to end Microsoft's operating system monopoly. Software could be written to operate based on the browser, rather than based on the Windows operating system.

[105] Microsoft's misconduct included acts such as i) imposing exclusionary terms in its agreements with manufacturers of computer hardware, internet service providers and internet content providers to keep rival browsers out of the major distribution channels, *id.* at 64–67, ii) threatening to withdraw technical support from Intel if the company continued to promote the rival browsers, *id.* at 77, and iii) intentionally deceiving software developers, causing the developers to write applications the developers thought would work outside of Windows when, in fact, the applications would only work with Windows. *Id.* at 76.

[106] *Intel Complaint*, *supra* note 102, at ¶¶ 2–28 (accusing Intel of engaging in monopoly maintenance in the market for, and of trying to leverage its dominance in CPUs into a monopoly over GPUs). CPUs act like the computer's "brain," integrating its many different functions. GPUs were initially sold as specialized integrated circuits for graphics processing, and interconnected with the CPU to perform this function. Because of this integration, Nvidia and other GPU manufacturers relied on "open interfaces" from Intel, consisting of both physical connections and programming, to enable their products to interoperate with Intel's CPUs. Eventually, the functionality of GPU's grew beyond just graphics and they threatened to turn from a complement into a substitute for CPUs. Intel then "beg[an] to perceive [GPU manufacturers] as a threat to its monopoly position in the relevant markets," *Id*. at ¶ 84, and allegedly used its monopoly power to delay this threat.

turned out to be incompatible with Intel's dominant CPUs.[107] Without accurate Intel interface information, GPU producers were left unable to design products that worked with—and competed as partial substitute against—Intel's dominant CPUs.[108]

Most importantly, each of these computing cases ended in a remedy that required the monopolist to provide its rivals with data access.[109] Microsoft was required to disclose its application programming interfaces ("APIs") and other technical information necessary for independent software to interoperate with Windows.[110] In particular, Microsoft was required to disclose APIs used by middleware, like web browsers, to access or call on "any services" in the Windows operating system, along with related documentation.[111] This included APIs that enabled the use of Windows functionality,

[107] *Id*. at ¶ 85.

[108] *Id*. at ¶ 22.

[109] The settlement agreements in the computing cases also included other obligations, but for the purpose of this discussion only the data access aspects of the remedies are described.

[110] *Microsoft*, 253 F.3d. at 99–100; United States v. Microsoft, No. 98-1232 (CKK) (D.D.C. Nov. 12, 2002) at *1, *modified and superseded* (Sept. 7, 2006), *further modified and superseded*, 2009 WL 1348218 (Apr. 22, 2009) [hereinafter *Microsoft Settlement Agreement*]. Although the government initially obtained a structural remedy to divide Microsoft into separate operating companies, this was overturned on appeal to the D.C. Circuit. Upon remand, the DOJ abandoned efforts to break up Microsoft. The case ended with a settlement agreement that imposed behavioral remedies, including the data access obligations discussed here. *See also* Press Release, Dep't of Justice, Justice Department Informs Microsoft of Plans for Further Proceedings in the District Court (Sept. 6, 2001), https://www.justice.gov/archive/opa/pr/2001/September/447at.htm (structural remedies not being pursued on remand); Press Release, Dep't of Justice, Department of Justice and Microsoft Corporation Reach Effective Settlement on Antitrust Lawsuit (Nov. 2, 2001), https://www.justice.gov/archive/atr/public/press_releases/2001/9463.htm [hereinafter *DOJ Microsoft Settlement Press Release*]. The parallel EU case against Microsoft also focused heavily on access and information remedies, *see* Eur. Comm'n, Commission Decision of 24 March 2004 Relating to a Proceeding Under Article 82 of the EC Treaty, Case COMP/C-3/37.792 – Microsoft, (Apr. 21, 2004).

[111] *Microsoft Settlement Agreement*, *supra* note 110, at III.D.

such as data storage or the use of fonts.[112] "Middleware," was so-called because it acted as a translation layer between the operating system and software running on that system. With guaranteed access to such APIs, software developers would be able to design software for non-Microsoft Internet browsers that still interoperated with, and thus offered the features of, the popular Windows operating system.

Further, Microsoft was required to disclose communication protocols for interoperation with its servers.[113] The protocols were sets of rules for exchanging information between the Windows operating system and a server operating system product connected via a network to the Internet (or another network).[114] Although server-based operating systems were not the subject of alleged misconduct in *Microsoft*, they posed an analogous threat to browsers, because such systems could also act as middleware. Like the APIs for browsers, the disclosed protocols enabled communication with Windows, and thus the creation of products that competed with Windows as a means of running software.

Antitrust enforcers expected that requiring Microsoft to disclose this interoperability data would "prevent recurrence of similar conduct in the future and restore competition in the software market."[115] By ensuring that developers had access to Windows APIs and other interoperability information, the DOJ sought to guarantee that competitors could offer server-based or browser-based experiences that emulated Windows functionality for consumers, and therefore provided robust competition for the Windows operating system. The hope was that Microsoft would no longer be able to quash competition by controlling interoperability with the dominant Windows.[116]

Though *Microsoft* is often held up as the leading example, technology monopolists both before and after Microsoft also faced data access remedies. In 1952, the DOJ

---

[112] *Microsoft*, 253 F.3d at 53 ("Windows contains thousands of APIs, controlling everything from data storage to font display.").

[113] *Microsoft Settlement Agreement*, *supra* note 110, at III.E.

[114] *Id*. at VI.B. (defining "Communications Protocol").

[115] *DOJ Microsoft Settlement Press Release*, *supra* note 110, at 1.

[116] *Id* at 2.

pursued a case against IBM that ended in a consent decree imposing data access obligations, among many other requirements.[117] IBM was ordered to supply the "technical information" necessary to use and manufacture its tabulating machines and cards.[118] To encourage competition in the aftermarket for service of used IBM machines, the company was also required to furnish independent maintenance service competitors with "copies of any technical manuals, books of instruction, pamphlets, diagrams or similar documents" provided to IBM's own employees for servicing IBM machines, in exchange for a reasonable, nondiscriminatory fee.[119]

Fast forward to 2010, and another technology monopolization case that ended in a data access remedy, this time against Intel. Intel was the subject of multiple government and private anti-monopolization cases for withholding technical interoperability information from rivals, in order to quash threats

[117] United States v. Int'l Bus. Machs. Corp., 857 F. Supp. 1089, 1090 (S.D.N.Y. 1994) (describing the timeline of the earlier case against IBM). Like Intel, IBM faced numerous interrelated antitrust cases.

[118] United States v. Int'l Bus. Machs. Corp., No. 72-344, 1956 U.S. Dist. LEXIS 3992, at *29–30 (S.D.N.Y. 1956) (ordering IBM to disclose technical information to the rivals that were also granted related compulsory intellectual property licenses). Although the many other obligations imposed on IBM are not discussed here, it is interesting that this manufacturing disclosure was combined with a conditional structural remedy. If IBM's market share did not decline below 50 percent of manufacturing capacity in the U.S. for tabulating cards, the consent decree provided for a potential structural remedy in the form of a divestiture. *Id.* at *18–20.

[119] *Id.* at *17. Similar disclosure was required of IBM to encourage competition in data processing services. *Id.* at *16 (ordering "upon written application and at reasonable and nondiscriminatory charges" that IBM disclose "any pamphlets, books of instruction or other similar documents which it furnishes to the Service Bureau Corporation relating to the operation and application of IBM tabulating or electronic data processing machines . . . ."). The Service Bureau Corporation was a wholly owned IBM corporation established by the consent decree in this case to hold separate all of IBM's contracts for data processing services. *See* Peter Passell*, I.B.M. and the Limits of a Consent Decree*, N.Y. TIMES (June 9, 1994), https://www.nytimes.com/1994/06/09/business/ibm-and-the-limits-of-a-consent-decree.html (explaining that companies would pay IBM to process payroll, bookkeeping or other data).

against its microprocessor monopoly.[120] One such case brought by the FTC against Intel in 2010 ended in a remedy that mandated access to Intel's technical data.[121]

This Intel settlement, like that in *Microsoft*, focused heavily on disclosure of company interoperability information. It required Intel to disclose an accurate version of its "interface roadmap" to the major manufacturers of GPUs.[122] The interface roadmap was an Intel corporate planning document that set out Intel's anticipated future microprocessor models, and the technical interface each model would require for a GPU to interoperate with it. The disclosure of this interface information was intended to enable GPU manufacturers to plan for their development and manufacture of GPUs that would be compatible with Intel's future CPU chipsets. This compatibility was seen as necessary for GPUs to be able to compete with Intel's dominant CPUs.

1. Digital Platform Monopolization Theories and Remedies Implicate Consumer Data

The remedies in *IBM*, *Microsoft* and *Intel* granted rivals access to "company" data, in the sense that the information was created, owned and exclusively controlled by the defendant corporation. The technology monopolist was ordered to disclose its own proprietary information. For IBM, this consisted of technical product design information and manuals. For Microsoft and Intel, it was the interoperability information for their respective products. In this sense, the nature of the data at stake in the computing cases was similar to that of other historical data access remedies that granted compulsory

[120] *See, e.g.*, Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1291 (N.D. Ala. 1998), *rev'd on other grounds*, 195 F.3d 1346 (Fed. Cir. 1999); Intel Corp., 150 F.T.C. 420 (Oct. 29, 2010); Intel Corp., 128 F.T.C. 213 (1999).

[121] Intel Corp., 150 F.T.C. 420 (2010).

[122] Decision and Order at VI.B, I.O, I.P, Intel Corp., 150 F.T.C. 420 (Oct. 29, 2010).

licensing of intellectual property,[123] access to know-how[124] or access to company databases.[125] All of these cases involved disclosure of corporate information.

How does the nature of the data in these historical cases compare to the information at stake in contemporary remedies? This requires identification of which data, exactly, is being sought from digital platforms. Unfortunately, demands that digital giants provide "data access" are often imprecise about this fundamental question. Herbert Hovenkamp criticizes the theories behind such demands as "opaque about specifics."[126] Technology giants collect, use and store all matter of data. Though necessarily influenced by the particulars of a given case,

---

[123] *See, e.g.*, Besser Mfg. Co. v. United States, 343 U.S. 444, 447 (1952) ("[C]ompulsory patent licensing is a well-recognized remedy where patent abuses are proved in antitrust actions and it is required for effective relief."); Crandall, *supra* note 44, at 116 (noting that 20.5 percent of civil cases through 1996 ended in compulsory licensing).

[124] A rash of Sherman Act cases in the 1950's imposed antitrust remedial orders that required companies to disclose their commercial expertise. United States v. United Shoe Mach. Corp., 110 F. Supp. 295, 354 (D. Mass. 1953), *aff'd per curiam*, 347 U.S. 521 (1954) (ordering a remedy that required "commercial practices" for shoe manufacturing be disclosed, along with compulsory licensing of manufacturing machines); United States v. Am. Can Co., 1950 Trade Cas. (CCH) 62, 679 (N.D. Cal.) (requiring defendant to disclose its technical information to those desiring to produce competing metal can manufacturing equipment, along with compulsory licensing); *see also* United States v. Gen. Elec. Co., 115 F. Supp. 835, 855 (D.N.J. 1953) (ordering the defendant "to furnish or make available to qualified applicants the 'know-how' of the manufacture of lamp machinery" as a remedy under Section 1 of the Sherman Act).

[125] *See, e.g.*, SolidFX, LLC v. Jeppesen Sanderson, Inc., 935 F. Supp. 2d 1069 (D. Colo. 2013), *aff'd*, 841 F.3d 827 (10th Cir. 2016) (seeking access to charts of airport topography); Nat'l Bus. Lists, Inc. v. Dun & Bradstreet, Inc., 552 F. Supp. 99 (N.D. Ill. 1982) (seeking access to a business credit information database). There are also a number of merger review cases where access to databases has been granted, though merger remedies are not addressed in this article. *See, e.g.*, Analysis of Agreement Containing Consent Order to Aid Public Comment, Nielsen Holdings N.V. and Arbitron Inc., File No. 131 0058 (Sept. 20, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130920nielsenarbitronanalysis.pdf.

[126] Hovenkamp, *supra* note 69, at 585; *see also* Tucker, *supra* note 67, at 6 ("In general, the debate about market power in online advertising tends to have a remarkable lack of precision.").

any meaningful discussion of data access remedies requires greater specificity about the type of data at stake.

It seems that the data demanded from digital platforms cannot be the same type of company information at issue in the computing cases. Unlike Microsoft and Intel, digital platforms like Facebook and Google already make their major APIs public for developers to access and use. Software developers can access and download APIs from the public website of each company.[127] Whatever "data access" is envisioned from digital platforms, this suggests the data is distinct in nature from computing cases past.

One point is clear—whatever data is being sought from digital platforms, those seeking access presumed that information is important in restoring competition. Restoration of competition is an animating goal of antitrust remedies. If access to the data is not important to competition, then there is no antitrust question.[128]

However, these observations do little to narrow the field of which data is assumed to be at stake in calls for access remedies. Technology giants are successful, at least in part, because they hold many different categories of competitively important data not available to their rivals. Their product designs, algorithms, employee know-how, trade secrets and more all contribute to their success. Assertions that access to data is necessary for competition with digital platforms could refer to any of these types of information. Access to each of these sources of data would be competitively significant for rivals, assuming an antitrust case could be made to obtain it.

---

[127] *See, e.g.*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/apis-and-sdks/#facebook-apis (last visited June 9, 2020) (describing how to access and use the Facebook Graph API and Marketing APIs); GOOGLE APIS EXPLORER https://developers.google.com/apis-explorer (last visited June 9, 2020) (listing available Google APIs).

[128] Many scholars argue precisely this in responding to monopolization theories, that data accumulation does not confer a competitive advantage, *see* sources cited at *supra* notes 66 and 67 (discussing the disagreement with data monopolization theories and sources).

The problem is that none of these types of data seem to fit with the liability theories driving calls for data access. The emphasis of such data monopolization arguments is on the anti-competitive harms that arise from the accumulation or "bigness" of data stores held by digital platforms.[129] The narrative of Stucke, Grunes and others is that the vast stores of data held by digital platforms are what confer a competitive advantage, as that data is used to exclude rivals from access to information necessary to compete.[130] The volume or amount of data is central to the theory of what renders it of competitive importance. By that logic, it cannot be information in the nature of product designs, algorithms or intellectual property at stake in calls for "data access" from digital platforms. These types of data typically draw value from their scarcity, not their accumulation.[131]

What type of data, then, is accumulated by digital platforms *en masse*, and is relevant to digital competition? The clearest answer is data about the online activities of consumers. Vast amounts of consumer data drive the new digital economy. In the last minute alone, Google fielded over 4 million user searches,[132] Facebook users uploaded almost 150,000 photos,[133] and Amazon sold up to 81,000 products.[134] Near-constant

[129] See discussion of these theories in the Introduction, *supra* Section I.B. *Introduction to Data Access Remedies and Digital Platform Monopolization Theories*.

[130] GRUNES & STUCKE, *supra* note 63; *see* discussion *supra* notes 63–65.

[131] Although patent portfolio accumulation is a potential competitive strategy, no such theory has been driving calls for access to digital platform data. Intellectual property has not played a particular significant role in competition with these companies.

[132] Domo, Inc., Data Never Sleeps 7.0, (last visited Aug. 11, 2020) https://www.domo.com/learn/data-never-sleeps-7 (reporting an average 4,497,420 Google searches per minute in 2019).

[133] Domo, Inc., Data Never Sleeps 8.0, https://www.domo.com/learn/data-never-sleeps-8, (last visited Aug. 11, 2020) (reporting that in 2020 to date, an average of 147,000 photos were uploaded to Facebook per minute).

[134] Lauren Thomas, *Amazon Says This Year's Prime Day Surpassed Black Friday and Cyber Monday Combined*, CNBC, July 17, 2019 (reporting 175 million items sold on Amazon during the 36 hour period of "Prime Day," a promotional event that typically reflects the highest volume

internet connectivity on a myriad of devices means data about these online activities of consumers is being produced at a velocity, volume and variety that has never been seen before.[135] As former FTC Chairwoman Edith Ramirez explains:

> "… each of us is generating data at an unprecedented rate. In fact, in 2013 it was reported that an astonishing 90 percent of the world's data was generated in the two preceding years. Today, the output of data is doubling every two years."[136]

Consumers actively provide their information to companies online through actions like entering data into forms, typing thoughts into a search engine, composing emails or posting content on social media. Consumers also provide massive amounts of data, often unwittingly, when their activities are tracked via online technologies like browser cookies and pixels. Virtually every online action can be traced, from a website visit, to a view of an ad or a product, placement or purchase of a product in an online shopping cart, and more. At the same time, near-constant connectivity through devices like smartphones enables tracking of consumer data such as user location or nearby devices, which can be cross-referenced with online information to learn more about that consumer.

Competition in social networking, online search, online shopping and a myriad of other digital services revolves around the collection, analysis and use of massive amounts of consumer data. Consumer data is the raw material driving the businesses of the largest digital platforms. The data gathered about consumers is used to "identify correlations, make predictions, draw inferences, and glean new insights" which are monetized in advertising and products, often targeted at that same consumer

---

period for Amazon sales each year). This amounts to approximately 81,000 products per minute during this period.

[135] Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 1–2 (2014).

[136] Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Sept. 15, 2014), https://www.ftc.gov/system/files/documents/public_statements/582421/140915bigdataworkshop.pdf (footnotes omitted).

who provided the data.[137] Almost every aspect of our online presence leaves a trail of data with potential commercial value. This value is evident from the revenue of Apple, Facebook, Amazon and Google, collectively over $690 billion in 2018—more than the annual GDPs of most national economies.[138]

For example, almost all of Facebook and Google revenue is generated from online advertising, which relies on the collection, use and analysis of data about consumers.[139] Facebook and Google operate as two-sided platforms in which one side delivers services, like search and social media, to consumers, while the other side sells advertising that relies on consumer data for ad targeting.[140] The two-sided nature of their business is what renders it viable. Consumer attention is drawn to the free services on one side of the platform. This attention in turn attracts the other side of the platform, the paying advertisers, who subsidize the consumer-facing services by paying for ads delivered to those same consumers.[141] The model is not unlike that of newspapers, wherein the news articles draw consumer attention, and advertisers are, as a result, willing to pay to place ads that make the newspaper financially viable.

In that sense, consumer attention and data have always had commercial value. Nielsen television viewership data has long been used to sell advertising. Loyalty cards have long been used to track and understand consumer buying behavior for marketing purposes. But never before has consumer data been monetized at such magnitudes and so profitably as it is today.

---

[137] *Id.*

[138] FREEMAN & SYKES, *supra* note 48, at 1.

[139] Facebook, Inc., Annual Report (Form 10-K), at 7 (Dec. 31, 2019) ("We generate substantially all of our revenue from selling advertising . . . ."); Alphabet, Inc., Annual Report (Form 10-K), at 29 (Dec. 31, 2019) (reporting $134.8 billion of revenue from advertising of $161.85 billion, amounting to approximately 83% of total revenues).

[140] For simplicity, these platforms are discussed here as two-sided. In fact, there are multiple "sides," depending on the specific business. For example, third-party application developers and advertising intermediaries also play an important role in the operation of many of these services.

[141] Some take issue with the description of these services as "free," characterizing payment as being in the form of consumer data, or user attention. *See generally* TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016).

As one author explains, digital platforms have "a type of personalized knowledge . . . that executives relying on old, analog Nielsen Ratings could never have dreamed of."[142] The fundamental nature of this shift in the economic role of data is evident in new terminology. Scholars have begun to refer to an "attention economy,"[143] a "data economy,"[144] or more critically, to "surveillance capitalism."[145]

The rise in the economic importance of consumer data has implications for data access remedies. Such remedies have always granted access to commercially valuable data, because their animating purpose is to restore competition. Competitors, and sometimes antitrust agencies, have consistently sought access to the competitively important information *du jour*. However, the nature of that data has shifted over time, from technical information about punch card computing in *IBM*, to know-how,[146] corporate databases,[147] and intellectual property,[148] then to software,[149] interoperability and technical information in cases like *Microsoft*[150] and *Intel*.[151] Cases against

---

[142] Pasquale, *supra* note 4, at 1024.

[143] Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 ANTITRUST L.J. 771, 771 (2019).

[144] Giuseppe Colangelo & Mariateresa Maggiolino, *Data Accumulation and the Privacy–Antitrust Interface: Insights from the Facebook Case* (TRANSATLANTIC TECH. L. FORUM WORKING PAPERS No. 31, 2018), at 2, https://law.stanford.edu/wp-content/uploads/2018/02/colangelo_maggiolino_wp31.pdf (describing the modern economy as the "data economy").

[145] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015).

[146] *See* cases cited at footnote 124.

[147] *See* cases cited at footnote 125; Corsearch, Inc. v. Thomson & Thomson, 792 F. Supp. 305, 306 (S.D.N.Y. 1992) (seeking access to databases of annotated state trademark cases).

[148] *See, e.g.*, Besser Mfg. Co. v. United States, 343 U.S. 444, 447 (1952) ("[C]ompulsory patent licensing is a well-recognized remedy where patent abuses are proved in antitrust actions and it is required for effective relief."); Crandall, *supra* note 44, at 116.

[149] Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1147 (1st Cir. 1994).

[150] *See* discussion *supra* Section III.A.1. *Digital Platform Monopolization Theories and Remedies Implicate Consumer Data*.

[151] *See id*.; *see also* Novell, Inc. v. Microsoft, 699 F. Supp. 2d 730, 736 (D. Md. 2010), *rev'd on other grounds*, 429 Fed. Appx. 254 (4th Cir. 2011); Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255 (N.D. Ala. 1998), *rev'd*

digital platforms will seek the newest incarnation of competitively important data. Unlike in *IBM*, or even *Microsoft* or *Intel*, this will now often be consumer information. Consumer information is fueling this generation of digital companies, and this means contemporary data access remedies are likely to involve that consumer data.

There is early evidence of this change in the nature of the data being sought in cases like *hiQ v. LinkedIn*[152] and *PeopleBrowsr, Inc. v. Twitter, Inc.*[153] Both cases involved allegations of unfair competition, and both resulted in interim injunctions that guaranteed competitors of the digital platform continued access to consumer information.[154] The injunctions required that LinkedIn and Twitter permit the plaintiffs to continue to access users' profiles and tweets, respectively. These cases, though preliminary rulings, are early indicators that it may well be consumers' online information at stake in the data access remedies granted against digital platforms.

---

on other grounds, 195 F.3d 1346 (Fed. Cir. 1999); Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1357–58 (N.D. Ala. 1998), *rev'd on other grounds*, 195 F.3d 1346 (Fed. Cir. 1999) (seeking pre-release product samples).

[152] 938 F.3d 985, 994 (9th Cir. 2019). LinkedIn is a digital platform for professional networking. Individuals post profiles with resume-like information and connect to others in a social network. In *hiQ v. LinkedIn*, the plaintiff, hiQ, was a competing data analytics firm that obtained an injunction to preserve its access to LinkedIn's user profile data. *Id.* at 991.

[153] No. C–12–6120 EMC., 2013 WL 843032 (N.D. Cal. 2013). Twitter is a social media platform on which individual users and corporations can post "tweets," which are short statements. PeopleBrowsr made its profit by providing data analysis of individual users' tweets. In exchange for $1 million in annual fees, Twitter gave PeopleBrowsr direct access to every individual users' tweets in real time. When Twitter threated to cut off PeopleBrowsr's access to this central feed of all user posts, PeopleBrowsr obtained a temporary restraining order that maintained its continued access to individuals' data. *Id.* at *1.

[154] *Id*.; 938 F.3d 985 (9th Cir. 2019). *But see* Stackla, Inc. v. Facebook Inc., No. 19-CV-05849-PJH, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019*)* (denying an injunction for plaintiff access to Facebook user data, as such a remedy "would compel Facebook to permit a suspected abuser of its platform and its users' privacy to continue to access its platform and users' data . . . issuing an injunction at this stage could handicap Facebook's ability to decisively police its social-media platforms in the first instance").

From a privacy perspective, this remedies shift from company data to consumer data is of fundamental relevance. Data privacy law had no relevance to the disclosure of company data in cases past. Now, data access remedies may well involve the information of individuals. This raises new questions around privacy of those individuals. Do consumers have privacy interests in the information that the monopolist is ordered to disclose?[155] If so, should the antitrust remedy be modified to accommodate those interests?

B. Consumer and Data Access Remedies that Predate the Rise of Data Privacy Law: The Telephone Directory Cases

This distinction between company and consumer data in historical cases begs the question: has *private* consumer data ever been ordered disclosed by a monopolization remedy? In short, yes, it has. This section considers a flurry of antitrust litigation in the late 1980s to early 1990s between phone service monopolists and their upstart rivals, who tried to obtain access to consumers' telephone directory listings ("the telephone directory cases").[156] At least one case granted the new entrants

---

[155] *See* discussion *infra* Section III.B.1.a. *Is the Competitively Important Data Held by Platforms Private?*

[156] Illinois Bell Tel. Co. v. Haines & Co., 683 F. Supp. 1204, 1205 (N.D. Ill. 1988), *aff'd*, 905 F.2d 1081 (7th Cir. 1990), *cert. granted, judgment vacated*, 499 U.S. 944 (1991); Great W. Directories, Inc v. Sw. Bell Tel. Co, 63 F.3d 1378, 1384-88 (5th Cir. 1995); Bellsouth Advert. & Publ'g Corp. v. Donnelley Info. Publ'g, Inc., 719 F. Supp. 1551 (S.D. Fla. 1988), *rev'd*, 999 F.2d 1436 (11th Cir. 1993)(reversing on copyright infringement claims only); Rural Tel. Serv. Co. v. Feist Publ'ns, Inc., 737 F. Supp. 610, 620 (D. Kan. 1990), *rev'd in part on other grounds*, 957 F.2d 765 (10th Cir. 1992); Directory Sales Mgmt. Corp. v. Ohio Bell Tel. Co., 833 F.2d 606 (6th Cir. 1987); White Directory of Rochester, Inc. v. Rochester Tel. Corp., 714 F. Supp. 65 (W.D.N.Y. 1989); Hutchinson Tel. Co. v. Fronteer Directory Co. of Minn., 4 U.S.P.Q. 2d (BNA) 1968, 1987 WL 14101 (D. Minn. 1987) [hereinafter, the "telephone directory cases"]. From an antitrust history perspective, these telephone directory cases are interesting because many of the defendants in the antitrust counterclaims were "baby Bells," whose monopolies over phone service were granted as a result of the structural remedy breaking up AT&T. *See, e.g*., *Bellsouth Advert. & Pub'g Corp*., 719 F. Supp. at 155; *Directory Sales Mgmt. Corp.*, 833 F.2d at 606 (bringing action against defendant Ohio Bell Telephone Co.).

access to consumer telephone listing data as part of the monopolization remedy.

However, as this section explains, these cases largely predate the rise of U.S. data privacy law. The cases therefore do not provide a full answer on how to address consumer privacy interests in the design of monopolization remedies. Despite this, the telephone directory cases offer a useful contrast to contemporary remedies, to illustrate the significant change in the legal landscape now implicated by the disclosure of private consumer data. The telephone directory cases also demonstrate that there is no principle within antitrust law that precludes the disclosure of information simply because it is about individual consumers and potentially private.

The best known of the telephone directory cases is *Feist Publications, Inc. v. Rural Telephone Service Co.*, in which the Supreme Court ruled on copyright claims,[157] but there were many similar suits that involved counterclaims of monopolization. The telephone directory cases involved disputes over access to consumer information held by telephone service monopolists, in the form of names, addresses and phone numbers used in telephone book listings.

Phone directories, like online search and social media, were two-sided platforms. The industry business model was to publish white pages listings of individuals' information for free, then earn revenue by selling yellow pages advertising in the same directories. One side drew consumer attention with free phone listings, and the other side subsidized that service with paid yellow pages advertising. The advertising drew its value from the consumer attention to phone listings.

The incumbent phone service companies were often endowed with a statutory monopoly over the provision of telephone services.[158] Because the incumbents were the sole

[157] 499 U.S. 340 (1991).

[158] In some cases, the statute also granted a monopoly over the issuance of telephone directories. The statutory nature of the monopoly is a fundamental difference from the alleged monopolies of digital platforms, and today would likely play a much larger role in similar cases than it did at the time of the telephone directory cases. Under the doctrine of implied

providers of phone services, they immediately knew the accurate listing data of each individual when he or she signed up for phone services, and could include that data in the incumbent's white pages directory.[159] The monopolists thus received privileged, complete, early and direct access to listing information through their mandate to provide phone service.

Each of the telephone directory cases involved a new, independent directory publisher trying to enter a phone directory market in competition with the local phone service incumbent. The new entrant would demand direct access to consumer's telephone listing data from the monopolist. The monopolist would refuse, at least on the terms that the entrant thought enabled it to compete. When the monopolist then published its public phone directory each year, the new entrants would, predictably, copy the listings information from it, and use that information for their own competing directories. In response, the monopolists would bring copyright infringement claims.[160] This pattern occurred so often that the incumbent monopolists even began seeding listings of fake individuals in their phone directories, to catch copying rivals in the act.[161]

The independent telephone directory company would then counterclaim under Section 2 of the Sherman Act, alleging the incumbent had monopolized or attempted to monopolize the business for yellow pages advertising through control of white pages listings. The central argument was that the independent publisher could not compete effectively in sales of yellow pages

---

immunity, when a monopolist's conduct is squarely subject to regulatory oversight and such regulation is incompatible with antitrust intervention, the activity is impliedly immune to antitrust law. Credit Suisse Sec. (USA) LLC v. Billing, 551 U.S. 264 (2007) (describing the factors used in determining the applicability of implied immunity); Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 406 (2004).

[159] Illinois Bell Tel. Co. v. Haines & Co., 683 F. Supp. 1204, 1205 (N.D. Ill. 1988), *aff'd*, 905 F.2d 1081 (7th Cir. 1990), *cert. granted, judgment vacated*, 499 U.S. 944 (1991).

[160] The Supreme Court eventually ruled there was no copyright in white pages listings in *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991).

[161] *See, e.g.,* Illinois Bell Tel. Co. v. Haines & Co., 905 F.2d 1081, 1085 (7th Cir. 1990), *cert. granted, judgment vacated*, 499 U.S. 944 (1991) (noting fictitious listings copied by a competing directory).

advertising, unless the monopolist directly provided direct and current listings data.[162] Although public white pages could be copied later (leaving aside the copyright disputes also raised in these cases), new entrants claimed the denial of a direct, up-to-date data source reduced the quality of their white pages listings, and made them less accurate and complete, which, in turn, rendered it difficult to attract yellow-pages advertisers in competition with the incumbent.[163]

In at least one of the telephone directory cases, *Great Western Directories, Inc. v. Southwestern Bell Telephone Co*.,[164] the antitrust plaintiff obtained a data access remedy.[165] The

[162] The independent publishers generally argued one or all of the following: (i) the white pages were an essential facility for competition in the yellow pages advertising market, to which the incumbent was refusing access, *see, e.g.*, *White Directory of Rochester, Inc.*, 714 F. Supp. 65 (alleging white pages to be an essential facility); *Ill. Bell Tel. Co.*, 683 F. Supp. 1204 (same); *Great W. Directories, Inc.*, 63 F.3d 1378 (same); (ii) by withholding the white pages data the incumbent was engaging in an unlawful refusal to deal, *see, e.g.*, *Feist Publ'ns, Inc.*, 737 F. Supp. at 620 (claiming a refusal to deal); *Bellsouth Advert. & Publ'g Corp.*, 719 F. Supp. 1151 (arguing a monopolization claim premised on a refusal to provide directory information); and/or, (iii) the incumbent was leveraging its monopoly over white pages listings to monopolize the yellow pages market, *see, e.g.*, *White Directory of Rochester*, *Inc.*, 714 F. Supp. 65; *Ill. Bell Tel. Co.*, 683 F. Supp. 1204; *Hutchinson Tel. Co.*, 1987 WL 14101, at *1; *Great W. Directories, Inc.*, 63 F.3d 1378. This reflects a similar mix of the anti-competitive conduct theories as those argued against digital platforms.

[163] For example, in *Feist*, the antitrust plaintiff claimed it was unable to provide complete listings without a direct license (despite copying) due to timing differences in publication of their directory, and changes in an estimated 30% of listings each year. Rural Tel. Serv. Co. v. Feist Publ'ns, Inc., 737 F. Supp. 610, 614 (D. Kan. 1990), *rev'd in part on other grounds*, 957 F.2d 765, 767 (10th Cir. 1992); *see* similar arguments in *Great W. Directories, Inc*., 63 F.3d 1378.

[164] 63 F.3d 1378 (1995) *withdrawn and superseded in part,* 74 F.3d 613 (5th Cir. 1996), *vacated pursuant to settlement* (Aug. 21, 1996). The subsequent withdrawal was regarding damages, not the injunction discussed here.

[165] The jury found the white pages listings data was an essential facility, to which access was required to compete in the telephone directory advertising market. The defendants violated Section 2 of the Sherman Act by denying the plaintiff directory publishers "reasonable" access to that data. *Great W. Directories, Inc.*, 63 F.3d at 1384 (describing jury verdict). The decision does not describe why the jury found that the competitors were unable to duplicate the listing data themselves, which is a required

District Court granted injunctive relief that required Southwestern Bell to license its white pages listings to the plaintiff, and the injunction was affirmed on appeal.[166] The injunction was strikingly prescriptive in nature. It required compulsory licensing of all current directory listings at a price of 13.5 cents per listing, plus an administrative fee of $500 per overall agreement and $25 per magnetic tape (the transfer mechanism).[167] Listings previously licensed could be reused in later directories with no additional licensing fee.[168] Any existing contractual terms inconsistent with the order were declared void.[169] Updates to the data could be obtained at the plaintiff's option, at the same 13.5 cent price.[170] Even future entrants to the same geographic market, who were not part of the case, were to be extended the same terms as provided in the injunction.[171]

The new entrants in *Great Western Directories* thus received access to consumers' data, consisting of names, addresses and phone numbers.[172] This was "consumer" data in

---

element of an essential facilities claim. *See* MCI Commc'ns Corp. v. Am. Tel. & Tel. Co., 708 F.2d 1081 (7th Cir. 1983). Southwestern Bell was also found to have violated Section 2 of the Sherman Act by monopolizing, and also of attempting to monopolize the market for telephone directory advertising, by leveraging its monopoly over the listings data and squeezing competitors' margins. *Id.*at 1385–86.

[166] 63 F.3d 1378 at 1390 (affirming District Court injunction after the jury finding of liability for Section 2 Sherman Act violations).

[167] Great W. Directories, Inc. v. Sw. Bell Corp., Civ. A. Nos. 2:88–CV–218–J, 2:89–CV–003–J, 1993 WL 755366, at *2 (N.D. Tex. Dec. 7, 1993), *aff'd in part, rev'd in part sub nom.* Great W. Directories, Inc., 63 F.3d 1378, *withdrawn and superseded in part*, 74 F.3d 613 (5th Cir. 1996), *vacated pursuant to settlement* (Aug. 21, 1996).

[168] *Id*.

[169] *Id*.

[170] *Id*.

[171] *Id*.

[172] It is fair to acknowledge that even if data privacy law had existed as it does now, there may have been some debate as to whether the directory listing information was subject to a reasonable expectation of privacy, given its quasi-public or even public nature in published directories. In *hiQ Labs, Inc. v. LinkedIn Corp.*, the Ninth Circuit was skeptical of continuing expectations of privacy in public information online, but also acknowledged "the fact that a user has set his [social media] profile to public does not imply that he wants any third parties to collect and use that data for all purposes." 938 F.3d 985, 994 (9th Cir. 2019) (quoting the district court decision). Since the information in the telephone directory cases included

that its nature was about individuals. The information disclosed in the remedy was, in that sense, similar to certain data accumulated by modern digital platforms, which relates to specific individuals. Certainly, the data looks quite different from the "company" information at stake in the computing cases, which involved technical standards and information unrelated to any individual consumer.

Despite the consumer-related nature of the data in the telephone directory cases, none of the decisions mention, much less consider, any potential consumer privacy interests in whether that data was sold or given to independent directory publishers.[173] There is no recognition, much less discussion, of whether consumers may want to prevent their listings from being used in rival directories, whether the defendant monopolist could withhold "unlisted" numbers from its data production under the remedy, or any means of transparency, data protection, limits on use or accountability for rivals who received and misused the consumers listing information. The remedy in *Great Western Directories*, for example, did not require any notice to consumers that if they signed up for phone service, their information would be provided to rival directory companies. There was no recognition of potential consumer privacy interests even when the new entrant publishers re-arranged and added to the data to provide further information about the consumer, such as listing by street address, the year the listing was last updated, the type of building at the address,

---

names, phone numbers and addresses, which are typically considered personally identifiable information, the better position is that consumers would have held a reasonable expectation of privacy in this data. Further, unlike the *HiQ* case in which consumers place the information online themselves, in the telephone directory cases there was no indication that consumers chose or even assented to publication of their information—publication seemed to be presented as a necessary corollary to phone service sign up.

[173] The closest hint of privacy being considered in the telephone directory cases was, ironically, in a case that involved business, not individual, information and thus no privacy interests. In *Bellsouth Advertising & Publishing Corp. v. Donnelley Information Publishing, Inc.*, the court observed "[t]his information is the same *non-confidential* business subscription information that Southern Bell provides to all similarly situated independent publishers." 719 F. Supp. 1551, 1553 (S.D. Fla.1988), *rev'd on other grounds*, 999 F.2d 1436 (11th Cir. 1993) (emphasis added).

demographic information, "and other useful information."[174] Instead, the dispute and remedies were framed as implicating only the directory publishers.

The simple explanation for this is, at the time the telephone directory cases occurred in the late 1980s to 90s, the concept of data privacy was not yet well developed in U.S. law. Although the right to privacy as Samuel Warren and Louis Brandeis envisioned it, the right to be "let alone," had existed for a hundred years in legal scholarship, the FTC's modern conceptions of consumer control over data were only beginning to emerge around the late 1990s.[175] The new common law of data privacy simply was not in existence at the time, and thus was not a consideration in the design of data access remedies. Nor would any of the sector-specific privacy legislation in the U.S. have applied to limit the disclosure of telephone directory data. The major difference between older data access remedies and those emerging for digital platforms, then, is not just the nature of the competitively important data at stake, but also that, for the first time, consumers may have legal interests in controlling that data.

1. The Rise of Data Privacy Law and its Application to Digital Platforms

Since the telephone directory cases, the legal landscape implicated by disclosure of private consumer data has changed dramatically. Over the last twenty-five years, the FTC has built up what Solove and Hartzog label "the new common law of privacy."[176] When the FTC took on its role as data privacy enforcer, as now, the U.S. had no omnibus protection of data

[174] *See* Ill. Bell Tel. Co. v. Haines & Co., 905 F.2d 1081, 1084 (7th Cir. 1990), *cert. granted, judgment vacated*, 499 U.S. 944 (1991) (detailing information in the directories).

[175] *See infra* Section III.B.1. *The Rise of Data Privacy Law and its Application to Digital Platforms*.

[176] Solove & Hartzog, *supra* note 72, at 583. The terminology stems from the tendency of FTC cases to end in settlement agreements, which, though not technically binding on third-parties, are carefully followed and highly influential, functioning in a role akin to common law.

privacy.[177] With the rise of the Internet in the mid-1990's, consumers were placing their data online in unprecedented amounts. The landscape of sector-specific privacy legislation in the U.S. left large swathes of this new online activity unprotected by any privacy laws.

Congress urged the FTC to fill this gap. Beginning around 1995, the FTC took up this challenge.[178] The agency engaged in a series of enforcement actions using its Section 5 FTC Act authority. Section 5 of the FTC Act grants the FTC the power to prevent acts or practices that are unfair or deceptive to consumers.[179] Through its enforcement actions, the FTC became the *de facto* regulator of personal data privacy in the U.S. Modern enforcement of data privacy law at the federal level is now synonymous with FTC action, taken either pursuant to sectoral privacy laws or Section 5 of the FTC Act.

The FTC's role in protecting data privacy evolved as a natural extension of its consumer protection law authority, much of which also relies on Section 5. At first, the FTC used its

---

[177] The default position in U.S. law is that data processing and uses are permitted, unless prohibited by piecemeal legislation or pursuant to the FTC's enforcement. This is a major difference from jurisdictions like the European Union, where the default position is the opposite; processing of personal information is *not* permitted absent a legal basis. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 881 (2014) (observing the distinction in default position for data processing in the U.S. compared to the EU); Charter of Fundamental Rights of the European Union art. 8 2012 O.J. (C 326) 391, 397 (describing individuals' fundamental rights to "the protection of personal data concerning him or her"); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

[178] Solove & Hartzog, *supra* note 72, at 598.

[179] 15 U.S.C. § 45(a) (2018). The FTC brings most of its data privacy cases under the "deception" 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 "unfairness" 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." Solove & Hartzog, *supra* note 72, at 598.

Section 5 power to enforce the promises companies made to consumers about privacy.[180] Companies faced FTC enforcement when they failed to uphold their privacy commitments to maintain consumer's data anonymity[181] or confidentiality,[182] to refrain from disclosing information to third parties,[183] or when they failed to limit data collection to what was described in their privacy policies.[184]

This early approach emphasized consumer notice and consent. Companies provided notice to consumers describing how their data was going to be collected, used, shared or sold, in privacy policies or other representations.[185] Consumers then choose whether or not to provide their consent for the described data-related activities. When companies did not provide

[180] Solove & Hartzog, *id.* at 648 (noting early FTC privacy actions based on companies failing to keep privacy promises).

[181] Complaint at 3–4, Compete, Inc., F.T.C. File No. 102 3155, No. C-4384 (Feb. 25, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf (company failed to remove personal information before transmitting data).

[182] Complaint at ¶ 6, Eli Lilly & Co., 133 F.T.C. 763, 766–67 (2002) (alleging violation of privacy agreement when Eli Lilly sent an email unintentionally disclosing personal information of consumers provided in conjunction with their website for anti-depressant drug Prozac).

[183] First Amended Complaint for Permanent Injunction and Other Equitable Relief at ¶¶ 17–18, Fed. Trade Comm'n v. Toysmart.com LLC, No. 00-11341-RGS, 2000 WL 34016406 (D. Mass. Jul. 21, 2000) (policy not to disclose personal information to third parties was violated upon sale of such information during bankruptcy).

[184] Complaint, Microsoft Corp., 134 F.T.C. 709, 715 (2002) (collecting information beyond what was disclosed in the privacy policy).

[185] The FTC's notice and consent model comes from the Fair Information Privacy Practices (FIPPS), an influential statement of basic protections for handling personal data. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (one of the earliest FTC forays into privacy analysis, emphasizing the FIPPS, and stating that the "most fundamental principle is notice . . . . The second widely-accepted core principle of fair information practice is consumer choice or consent."); U.S. DEP'T OF HEALTH, EDUC., & WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) (first articulation of the FIPPS).

adequate notice or failed to obtain sufficient consent for their collection and use of private data, they risked FTC enforcement.

The FTC has since expanded its enforcement efforts, increasing its focus on protection of consumers' reasonable expectations of privacy.[186] Under this view, consumer harm arises from the violation of reasonable expectations of privacy. Such expectations are not necessarily tied to whether a company failed to uphold a privacy promise. This shift is significant, because it moves U.S. data privacy law toward baseline data privacy protections.[187] Even if a customer checks a box to indicate formalistic consent, when the terms or the presentation of the terms are at odds with consumer expectations, the FTC could still pursue action against the company.[188] As discussed below, this shift also has significant implications for the accommodation of data privacy within antitrust remedies.[189]

a. Is the Competitively Important Data Held by Platforms also Private?

These changes in the landscape of data privacy law create a new question for monopolization remedies: is the consumer data at stake in data access remedies also subject to data privacy protection?

The sectoral privacy laws in the U.S. do not apply to much of the data held by digital platforms. Those laws apply only to specific types of data and certain entities.[190] Therefore,

---

[186] Solove & Hartzog, *supra* note 72, at 661.

[187] *See id.*

[188] *Id.* at 667 (noting the FTC's baseline standards approach "taking consumers as it finds them, full of preexisting expectations, contextual norms, and cognitive limitations, and prohibiting companies from exploiting these assumptions and rational ignorance").

[189] *See infra* Section III.B.1.b. *The Emergence of Co-Control of Data Creates Challenges for Antitrust Remedies.*

[190] Solove & Hartzog, *supra* note 72, at 587 ("[T]here is no federal law that directly protects the privacy of data collected and used by merchants such as Macy's and Amazon.com. Nor is there a federal law focused on many of the forms of data collection in use by companies such as Facebook and Google."). Technology companies are not, for example, financial institutions, the trigger for obligations under the Gramm-Leach-Bliley Act, nor is much of the information health data such that it might trigger HIPAA

to the extent there are consumer expectations of privacy recognized in the data held by digital platforms, it is likely to be pursuant to the FTC's general Section 5 FTC Act authority.

The FTC's use of Section 5 for data privacy enforcement originated with, and continues to focus on, protecting the online personal information of consumers.[191] As discussed above, the FTC's earliest forays into data privacy enforcement were closely tied to the dramatic rise of the Internet and e-commerce, which caused consumers to place their data online in unprecedented amounts beginning around the mid-1990s.[192] The FTC took on its data privacy protection authority to address Congressional concerns that consumers and their online information were otherwise unprotected in law.

In the time since, FTC privacy enforcement reads like a history of consumer data driven companies. The FTC initially took action against the social networking company MySpace,[193]

---

protections. *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered titles of 5, 8, 10, 18, 22, 25, 29, 31, 38, 42 U.S.C.). State data protection laws or emerging state data privacy legislation like that in California may apply to data held by digital platforms, but that is beyond the scope of this article, which focuses on the federal data regime. *See, e.g.*, The California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (2018). If anything, as state data privacy protection expands it could raise similar tension with antitrust law remedies to that discussed with regard to federal data privacy law here.

[191] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2019, at 2 (2020), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[192] *Prepared Statement of the Federal Trade Commission on Consumer Privacy Before the Comm. on Com., Sci,, and Transp.*, 112th Cong. 2 (2010) (statement of Jon Leibowitz, Chairman, FTC), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy/100727consumerprivacy.pdf ("With the emergence of the Internet and the growth of electronic commerce beginning in the mid-1990s, the FTC expanded its focus to include online privacy issues.").

[193] Complaint at 5–6, In re MySpace LLC, No. C-4369 (F.T.C. Aug. 30, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf (noting that MySpace deceptively failed to disclose to users

then Twitter, [194] and more recently, Google[195] and Facebook.[196] In fact, the FTC has pursued Facebook multiple times for data privacy violations.[197] Digital platforms are at the center of FTC data privacy enforcement. This focus on digital platforms in FTC cases suggests consumers have expectations of privacy in at least some of data held by these platforms. If they did not, these digital companies would not feature so heavily in the FTC's historical and current privacy enforcement.

---

of its online social networking service that it was sharing information with third parties).

[194] Complaint, Twitter, Inc., F.T.C. No. 092-3093, 2010 WL 2638509 (F.T.C. 2010), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf (finding that Twitter, a popular social media service, deceived customers when it failed to honor user choices to designate certain "tweets" as private). The case ended in a settlement agreement. Decision and Order at 4, Twitter, Inc., F.T.C. No. 092-3093, 2011 WL 914034 (Mar. 2, 2011).

[195] Complaint for Civil Penalties and Other Relief, United States v. Google, Inc., No. CV 12-04177 HRL (N.D. Cal. Nov. 20, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf.

[196] Agreement Containing Consent Order, Facebook, Inc., No. 092 3184 (F.T.C. 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf.

[197] In 2019, the FTC obtained a record setting fine against Facebook again for a violation of the order in an earlier case. Facebook had allowed a third party, Cambridge Analytica, to use a Facebook API to access the information of Facebook users without adequate consent. The Facebook API settings permitted access not only to the profiles of users of the application, but also access to the data of friends of the user in the same social network. The app harvested the data of an estimated 50 million Facebook users, but only 270,000 users had actually consented to access. Order Modifying Prior Decision and Order, Facebook, Inc., No. C-4365 (F.T.C. Apr. 27, 2020), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf; Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html. For a detailed description of the Cambridge Analytica scandal, *see* Matthew Rosenberg *et al*., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

The FTC considers information that is personally identifiable to be private, but defines that concept broadly in scope.[198] Personally identifiable information is viewed as including not just data about an individual, but also data that is "reasonably linkable" to an individual, or their electronic device.[199] For this reason, one FTC Chairman explained, "you can't focus on traditional notions of [personally identifiable information] such as name and address, when particular devices—and even consumers—are so readily identifiable without it."[200] The agency has pursued cases against digital platforms for constructive sharing of personal information when non-personal information was shared but that data could be identified back to an individual.[201] The more data that is collected about an individual, the more likely that information can be cross-referenced to identify him or her.[202] On this basis,

---

[198] The concept of personally identifiable information ("PII") is often the trigger for protection of data privacy, particularly in the application of sectoral privacy laws. PII is often protected by such legislation, while non-PII is left unprotected. The problem is that PII is often defined circularly, as data identifiable to an individual. For example, the Children's Online Privacy Protection Act identifies "personal information" as "individually identifiable information about an individual collected online," then lists specific categorical examples like name and email address. 15 U.S.C. § 6501(8) (2018).

[199] Complaint, In re MySpace LLC, No. C-4369 (F.T.C. Aug. 30, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf [hereinafter, *Myspace Complaint*] (FTC action against MySpace for sharing "MySpace IDs," an identifier assigned to each user, because that data could be easily traced back to consumers personal information).

[200] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks: FTC Privacy Roundtable, at 3 (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf.

[201] *MySpace Complaint*, *supra* note 199.

[202] Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (cross-referencing app location data to identify employees of the Mayor of New York and also a 46-year-old math teacher, based on visits to her work, dermatologist and ex-boyfriend's home); Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=al

the FTC has been broad in its inclusion of data considered to be personal and private, including geolocation information, email addresses and "persistent identifier[s]," like Internet Protocol (IP) addresses, mobile device IDs and unique customer numbers held in a cookie.[203]

These are the same types of consumer data that drive digital platform businesses. Similar categories of personally identifiable information are commonly used by digital platforms and advertisers to track, analyze and monetize consumer online activity.[204] Many types of commercially important data held by digital platforms are thus also likely to be personally identifiable, and subject to reasonable expectations of privacy. For example, the FTC has categorized Facebook user profile information as "personal information."[205] Recent tort litigation has similarly suggested that reasonable expectations of privacy are plausible in the user data gathered via browser cookies, and in the browsing history held by Facebook and Google.[206] This is the same data used to deliver targeted online advertising that makes up almost all of the revenue of these digital platforms.

For the first time, this creates the very real possibility of overlap between the data that is considered private, and the data

---

l&_r=0 (explaining that reporters were able to identify Thelma Arnold, a 62-year-old widow who lives in Lilburn, Georgia as AOL searcher 'No. 4417749' from the content of her online searches and other data).

[203] *See, e.g.*, Consent Order at 5, Unrollme Inc., File No. 172 3139 (F.T.C. Dec. 16, 2019), https://www.ftc.gov/system/files/documents/cases/c-4692_172_3139_-_unrollme_order.pdf (defining these categories as included in personally identifiable information).

[204] *See supra* Section III.A.1. *Digital Platform Monopolization Theories and Remedies Implicate Consumer Data*.

[205] Complaint at ¶ 1, Cambridge Analytica, LLC, Docket No. 9383 (F.T.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf (alleging deceptive acts or practices in gathering Facebook user profile information).

[206] *In re* Facebook, Inc., 956 F.3d 589, 603 (9th Cir. 2020) (finding plaintiffs adequately alleged a reasonable expectation of privacy in light of Facebook's widespread, "surreptitious and unseen" collection of data through the use of cookies after a user logged out of Facebook); *In re* Google, 806 F.3d 125, 129, 151 (3d Cir. 2015) (finding users maintained a reasonable expectation of privacy in their browsing histories).

that drives competition. Recent theories of monopolization harm levied against digital platforms emphasize the competitive value of accumulated data. For digital platforms, such data will often be consumer information.[207] If access to the private data of consumers is necessary to restore competition, then antitrust remedies are faced with how to address data privacy.

This is not to say that all of the consumer data held by digital giants is private, personal information. Some of the data is designed for public consumption, like publicly shared social media posts, though consumers may still have privacy interests in controlling the specific audience for those posts. Other data is aggregated or anonymized such that it is not identifiable to an individual, and it may not implicate data privacy interests.

It is possible that cases against digital platforms may involve this sort of non-private consumer data. However, the boundary between private and non-private data is not yet well defined, particularly online. For example, there are indications that "anonymized" data can be shockingly re-identifiable when cross referenced with other information.[208] The parameters of consumers' reasonable expectations of privacy are still developing in data privacy law. Though it would be wrong to categorize all consumer data held by digital platforms as private, the FTC's historical and current enforcement efforts against digital platforms make it seem equally incorrect to deny that any data privacy interests subsist in that information. More than ever before, it is likely that competitively important data will also be subject to consumer data privacy interests. Antitrust theory has yet to consider the impact of this new reality on remedies.

---

[207] *See supra* Section III.A.1. *Digital Platform Monopolization Theories and Remedies Implicate Consumer Data*.

[208] Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC's Action against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 6 (2009); EXECUTIVE OFFICE OF THE PRESIDENT PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 39 (May 2014) ("Anonymization . . . is not robust against near-term future re-identification methods . . . sometimes giving a false expectation of privacy . . . ."), https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

b. The Emergence of Co-Control of Data Creates Challenges for Antitrust Remedies

If the data disclosed pursuant to remedies is private, that creates a new challenge for remedies related to co-control. The application of data privacy law will split control over competitively important data between the defendant and the consumer, in a way antitrust remedies have never faced before. In antitrust remedies past, the monopolist was the only party to exercise control over the data ordered to be disclosed. In *IBM, Microsoft*, *Intel* and the telephone directory cases, it was entirely within the power of the defendant to grant access to the subject data. The data was proprietary information in the computing cases, which meant the company had exclusive power over that information. The data was owned by the monopolist. Even in the telephone directory cases, which involved consumer phone listing data, consumers had no legally recognized privacy interests in the data subject to remedial access. There was no consumer control over the information at stake in the remedy. In reaching a settlement agreement, the defendant company in each of these cases could freely agree to relinquish its control to the extent necessary to satisfy the antitrust agency or court.

The challenge now is that the FTC's common law of data privacy is rooted in consumer control over personal information.[209] Control is central to the conception of data privacy.[210] Warren and Brandeis's classic and influential

[209] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS at 10 (Mar. 2012) (describing "consumer control" as a principle embodied in the FTC's enforcement framework) [hereinafter FTC PROTECTING CONSUMER PRIVACY REPORT]; Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 972 (2017) ("Control has become the archetype for data protection regimes."); Dennis Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 449 (2020) (identifying Westin's work as underlying modern privacy legislation and regulation).

[210] This implicates the broader question of what privacy is, which is among the most divisive and slippery concepts in legal scholarship. Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J.

conception of the "right to be let alone"[211] argued for legal recognition of a right to privacy by analogy to the common law control authors and creators held over publication of their works.[212] Influential later scholarship such as Alan Westin's 1967 book, *Privacy and Freedom*, conceived of a right to privacy as control over one's information, describing "the right of the individual to decide . . . when and on what terms his acts should be revealed to the general public" with "only extraordinary exceptions in the interests of society."[213]

As Paul M. Schwartz observes, the conception of privacy as control has become the dominant theory of informational privacy.[214] From the earliest federal privacy statute in the U.S.,[215] to the most recent legislation and conceptions of user data privacy rights,[216] data privacy continues to be framed in

385, 406 (2015) ("Privacy theorists differ famously and widely on the proper conception of privacy . . . ."); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479–80 (2006) (canvasing scholarship describing privacy and finding "an embarrassment of meanings"). This article does not opine on the propriety of conceiving of informational privacy as control over data, but rather observes that such a conception lies at the core of the FTC's enforcement of data privacy.

[211] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting Thomas M. Cooley, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (Chicago, Callaghan & Co. 2d ed. 1888)).

[212] *Id*. at 199-200 ("the individual is entitled to decide whether that which is his shall be given to the public… the common-law protection enables him to control absolutely the act of publication…").

[213] ALAN WESTIN, PRIVACY AND FREEDOM 46 (1967) [hereinafter WESTIN].

[214] Fairfield & Engel, *supra* note 210, at 408 (citing WESTIN and others, noting "[t]he weight of the consensus about the centrality of privacy-control is staggering"); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

[215] The Fair Credit Reporting Act of 1970 limits the access of third parties to credit data, except for a set of permissible purposes. 15 U.S.C. § 1681b (2018).

[216] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 260 (2013) ("Legal frameworks all over the world continue to emphasize consent, or individual control, as a fundamental principle of privacy law."); Margrethe Vestager, Comm'r of Competition, Eur. Comm'n., Making Data Work for Us, Speech at Data Ethics Event on Data as Power (Sept. 9, 2016), https://wayback.archive-it.org/12090/20191129211903/https://ec.europa.eu/commission/commission

terms of control of information. The Supreme Court confirms that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[217] When the FTC pursues digital platforms, it is often for misrepresentations regarding consumers' control over their data.[218] The conception of privacy as control thus pervades legislative, judicial, policy and regulatory approaches to data privacy.

For antitrust remedies, the control paradigm that permeates U.S. data privacy law means that personal data subject to antitrust remedies is no longer within the monopolist's exclusive legal or practical control. In a post-data privacy law world, access to online user data is often co-controlled by the individual user and by the digital platform.

Consider, for example, third-party access to an individual's social media profile on Facebook. Facebook determines the technical API permissions that dictate, on a technical level, the consumer information available to third-party applications interconnecting with Facebook. The Facebook Graph API is an example of this, and is used by apps to access consumers' profile pictures, email addresses, friends lists and posts.[219]

However, layered on top of these API permissions are consumer privacy settings. These account or app-specific

---

ers/2014-2019/vestager/announcements/making-data-work-us_en ("The new General Data Protection Regulation will give us better control of our personal data."); The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 11 (Feb. 2012), https://www.hsdl.org/?abstract&did=700959 (proposing a Consumer Privacy Bill of Rights that includes "individual control" as a basic principle).

[217] U.S. Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1988).

[218] *See, e.g.*, FED. TRADE COMM'N, *supra* note 191 (describing an FTC case against Facebook for "misrepresenting the control users had over their personal information").

[219] FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/graph-api/faq (last visited June 9, 2020).

settings enable individual users to control access to certain data on their Facebook profiles. The consumer can use his or her settings to choose who can access certain information. This might include permitting a given app to see their email address, but not their friend list. At the account level, consumers might use their settings to determine a default audience for certain social media posts, or to limit who has access to their birth date. If the consumer chooses to deny access to applications through the use of such settings, the API's technical permissions become moot, overruled by that consumer's choice. Access to the private information of users on digital platforms thus depends on a blend of technical permissions controlled by the platform and settings controlled by the individual or individuals who have privacy interests in the data.

The conception of privacy as control creates tension with a remedy that purports to override such consumer settings, or expectations, regarding access to personal information. If , in the scenario above, Facebook or third-party applications disregarded the consumer privacy settings, or if the settings (or related disclosures) were unfair or deceptive in portraying the level of privacy afforded, the companies would risk FTC data privacy enforcement[220] and even scrutiny from Congress.[221] Consider that the FTC pursued Google for gathering data in

[220] *See, e.g.*, Order Modifying Prior Decision and Order, Facebook, Inc., No. C-4365 (F.T.C. Apr. 28, 2020), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf (order and consent to modify prior FTC order against Facebook, alleging Facebook violated the prior FTC order by misrepresenting both "the extent to which users could control the privacy of their data" and "the information [Facebook] made accessible to third parties"). This complaint and order modification arose because Facebook permitted Cambridge Analytica's third-party application to access data located on the profiles of individuals who had not themselves downloaded the application. *See* sources at *supra* note 209.

[221] *See generally Facebook, Social Media Privacy, and the Use and Abuse of Data*: *Joint Hearing Before the S. Comm. on the Judiciary and Sen. Comm. on Commerce, Science, and Transportation*, 115th Cong. (Apr. 10, 2018) (testimony of Mark Zuckerberg, Facebook, Inc. Chief Executive Officer); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce*, 115th Cong. (Apr. 11, 2018) (same).

violation of user data privacy settings,[222] and brought enforcement against Facebook for making deceptive representations about users' ability to rely on such settings to control who sees their profile information.[223] These cases indicate the FTC expects digital platforms to honor user privacy settings as an obligation under the new common law of data privacy. Yet in a recent antitrust case, the interim remedy granted access to the profile data of individuals on LinkedIn in violation of their user account settings.[224] In *HiQ v. LinkedIn*, LinkedIn users could activate a setting on their profile called "do not broadcast." When activated, the setting prevents any changes the user makes to profile information from being broadcast out in messages to each person in the user's LinkedIn network.[225] LinkedIn is a professional networking platform, which means profile updates could indicate the user is looking for a new job. The plaintiff, HiQ, sells data analytics software that scrapes user profiles to identify changes. HiQ's software then effectively contravenes the LinkedIn users' "do not broadcast" settings, by alerting employers to changes in their employees' profiles, to help identify employees at risk for leaving their company.

The Ninth Circuit expressed skepticism over whether users held privacy interests in their public LinkedIn profile data,[226] despite the "do not broadcast" setting. The Court upheld a preliminary injunction that required LinkedIn to allow HiQ to

---

[222] 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 (considering Google's privacy settings for users and instructions on how to use those settings and arguing that Google inaccurately represented to users whether its Safari browser was tracking their online activity through cookies, a digital tracking technology used to deliver advertising).

[223] 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 (finding Facebook deceived users with privacy settings on their social media service that gave users an inaccurate impression that they could control who accessed their social media profile).

[224] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 990 (9th Cir. 2019).

[225] *Id*.

[226] *Id*. at 994 (finding it "doubtful" that LinkedIn users "maintain an expectation of privacy with respect to the information that they post publicly").

continue to access consumer profile data, regardless of user data privacy settings.[227] Even if consumers choose the "do not broadcast" setting for their LinkedIn profile, HiQ can contravene that setting and disseminate information that highlights consumers' profile changes.

If LinkedIn itself had chosen to ignore the "do not broadcast" setting to offer its own software like that of HiQ, then LinkedIn could easily have faced Section 5 FTC Act enforcement for unfair or deceptive misrepresentations regarding that setting. The effect on consumer privacy looks much the same whether LinkedIn ignores user settings or a data access remedy ignores user settings. Either way, a rival of the digital platform, with whom the consumer likely has no prior relationship, gains access to that consumer's personal information, without permission. The difference between the data access remedy and the data privacy law prohibition is the existence of the remedial order.

The new reality for antitrust remedies is that, with the rise of data privacy law, the monopolist and individual users may both exert control over consumer data. If that consumer information is essential to competition (as those demanding data access remedies assume), then data privacy and data competition are in tension. The privacy and competition interests are left unreconciled at a theoretical or policy level. If the same platforms and the same information are subject to access demands in the name of competition, and insistence on data protection, how do we reconcile the two? In such situations, are consumers better off with greater data competition or greater data privacy?

[227] *Id*. at 1005 (affirming preliminary injunction); *But see* Stackla, Inc. v. Facebook Inc., No. 19-CV-05849-PJH, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019) (finding a public interest in "Facebook's protection of its users' privacy" where Facebook terminated a third-party app's access to user data on the social media service; denying a preliminary injunction to restore that access).

IV. PROPOSAL: TOWARD A RECONCILIATION OF DATA PRIVACY AND MONOPOLIZATION REMEDIES

In sum, older monopolization cases did not have any need to consider data privacy. Some cases predated the rise of data privacy law, while others involved only company data, the disclosure of which did not implicate the privacy of individual consumers. This has changed for remedies against digital platforms. Now, consumer data plays a significant role in digital competition. Swathes of competitively important data are now also subject to data privacy interests and protection. For data access remedies, these changes create unexamined complexity, particularly around co-control of data by monopolists and consumers. Yet existing theories on the intersection of antitrust law and data privacy do not address remedies.

This article calls for antitrust analysis to consider data privacy in the design of data access remedies, particularly for digital platforms. Courts and agencies should analyze whether consumers hold reasonable expectations of data privacy in the information subject to the remedy.[228] If so, what are the tradeoffs

[228] Specifically, agencies could include consideration of data privacy in their policy work on remedies, in crafting requests for relief in litigation and their negotiation of settlement agreements. For courts, such consideration could involve an assessment of relevant data privacy interests as part of the analysis of the "public interest" factor considered in granting injunctive relief. Cases outside of the antitrust context have taken data privacy into account as part of the public interest assessment, as well as under the irreparable harm factor. *See, e.g.*, Stackla, Inc. v. Facebook Inc., No. 19-CV-05849-PJH, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019) (denying injunction to maintain plaintiff's access to user data on Facebook, finding "the public has a strong interest in . . . Facebook's protection of its users' privacy" based on FTC and Congressional action to police privacy on Facebook); Domain Name Comm'n Ltd. v. DomainTools, LLC, 781 Fed. App'x 604, 607 (9th Cir. 2019) (finding no abuse of discretion where the lower court considered data privacy of domain registry users within its assessment of the public interest factor); Kaplan v. Bd. of Educ. of City Sch. Dist. of City of New York, 759 F.2d 256, 259–60 (2d Cir. 1985) (considering appellant's claim of irreparable harm "based on their fear that forced disclosure [of financial data] will allow personal and confidential information to be released to the public and the press," but finding safeguards put in place were sufficient to protect privacy). *See generally*, Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 20 (2008) (explaining several factors to be considered in granting a preliminary injunction,

between protecting such expectations and restoring data-driven competition?

Consider the alternative of ignoring data privacy at the remedies stage. If data privacy is left out of the analysis, antitrust remedies may unwittingly fail to increase consumer welfare. Such a remedy would undermine the consumer welfare purpose of bringing the antitrust enforcement action.[229] FTC data privacy enforcement is premised on the view that data privacy incursions, such as the unauthorized collection, use or sale of personal data, cause harm to consumers.[230] In fact, the FTC's authority to bring unfairness cases under Section 5 of the FTC Act requires that an act or practice is likely to cause "substantial injury" to consumers, or cause "detriment" to consumers in deception cases.[231] An antitrust data access remedy could require a defendant to grant rivals the ability to collect, use or even sell the private data of consumers, without consumer consent. The effect on consumers of such a remedy looks much like the effect of a data privacy incursion.[232] Assuming the premise of FTC privacy enforcement is correct—that consumer

---

including that the plaintiff is "likely to suffer irreparable harm in the absence of preliminary relief. . . and that an injunction is in the public interest").

[229] *See generally* Waller, *supra* note 25.

[230] *See, e.g.*, Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n, The Near Future of U.S. Privacy Law, Remarks at the University of Colorado Law School, at 7 (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf (describing use of Section 5 FTC Act authority "routinely" to prevent practices that "harm consumers, such as . . . data tracking without consumer consent"); FTC PROTECTING CONSUMER PRIVACY REPORT, *supra* note 209 at 9 (describing the evolution of the FTC's privacy enforcement "to include a focus on specific consumer harms as the primary means of addressing consumer privacy issues," which meant targeting practices that caused "unwarranted intrusions in [consumers'] daily lives," or physical or economic harm).

[231] 15 U.S.C. § 45(n) (2018) (unfairness); Solove & Hartzog, *supra* note 72, at 628 (describing elements of a deception claim).

[232] To be clear, the suggestion is only that the effect on consumers seems similar. This is not meant to imply that the FTC Bureau of Consumer Protection would pursue a data privacy case against a defendant who was ordered to disclose information pursuant to an antitrust remedy. That sort of direct antitrust law and data privacy law conflict is highly improbable and unrealistic, even where the remedial disclosure is inconsistent with the defendant's past privacy representations to consumers.

harms arise from privacy incursions—this means the antitrust remedy could itself cause consumer privacy harm.[233]

Unless and until that potential consumer privacy harm arising from the remedy is considered, it is unclear whether the remedy improves consumer welfare. The harms to data privacy could outweigh the benefits to consumers achieved from remedy-driven competition. In that case, the net result of the antitrust enforcement is to leave consumers worse off. Ignoring data privacy at the remedies stage risks this scenario. Alternatively, the benefits to consumers from remedy-driven competition may outweigh any privacy harms. [234] In that scenario, overall consumer welfare is improved by the antitrust remedy.

Without the added step of considering privacy impacts from the remedy, we cannot know which of these scenarios is occurring.[235] Put simply, "a bad Section 2 remedy risks hurting consumers."[236] Right now, the antitrust analysis does not check

---

[233] Some authors raise a fundamentally more skeptical view, questioning whether the FTC's data privacy law enforcement advances consumer welfare, or at least whether there is sufficient explanation and economic analysis by the FTC to prove that this is true. *See, e.g.*, James C. Cooper & Joshua Wright, *The Missing Role of Economics in FTC Privacy Policy*, CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 465, 485 (2018) (calling into question whether data privacy enforcement improves consumer welfare; arguing the FTC has largely assumed its privacy enforcement action benefits to consumer welfare instead of robustly analyzing using economic principles). This article is not so skeptical, and accepts for the purposes here that the FTC is fair in its view that its enforcement efforts under Section 5 of the FTC Act are positive for consumers.

[234] A third, if seemingly less likely, possibility is a precisely equal impact on consumer welfare from the privacy and competition-related effects. In that case, the cost of imposing the remedy would be a waste, since no remedy at all would have the same (lack of) net effect. Such a scenario could be treated the same way as a decline in consumer welfare.

[235] *See, e.g.*, Julie Brill, *Competition and Consumer Protection: Strange Bedfellows or Best Friends?*, ANTITRUST SOURCE, Dec. 2010, at 3 ("[B]efore competition principles can trump consumer protection concerns, any legitimate consumer protection issues must be identified and balanced against the competitive harm.").

[236] *See, e.g.*, Barnett, *supra* note 2, at 32.

whether the remedy is "bad" from the perspective of potential privacy harm arising from the remedy itself.

This argument takes an integrationist view of consumer welfare, in that it considers data privacy harms within its assessment of consumer welfare. Integrationists have already called for antitrust liability-stage analysis to consider privacy-as-quality harms to competition. This proposal extends similar thinking to remedies, but with the added acknowledgement that the privacy harms could differ between the liability and remedies stages of a case, as discussed below.[237]

However, this proposal may also offer common ground with separatists in the debate over data privacy and antitrust law. Though separatists dismiss privacy as beyond the scope of antitrust analysis, this insistence is driven by concern that expansion of the consumer welfare standard will dilute and disorganize antitrust analysis.[238] The separatists contend that if antitrust law is expanded to encompass other interests like data privacy, then consumer welfare will no longer function as the guiding star in cases. It could become unclear which factor to prefer if the effects on data privacy are at odds with price effects or other aspects of competition, and therefore uncertain which conduct to condemn in antitrust law. However, this dilution concern is expressed with regard to liability analysis of harms, not theories of remedies.

Even the separatist view leaves room for this proposal to consider data privacy in the design of remedies, because this approach can be implemented without expanding the consumer welfare conception applied in the liability analysis. It is possible that the traditional conceptions of consumer welfare could be retained in the analysis of liability, and also that privacy impacts could be considered at the remedies stage. It is not uncommon in other areas of law, and in existing antitrust law, for distinct considerations to arise in the analysis of liability and the

[237] *See infra* Section IV.A. *Implementing the Proposal*.

[238] *See supra* Section II.A. *The Separatists: Data Privacy is Beyond the Purview of Antitrust Law*.

adjudication of remedies. These different stages of a case often necessitate analysis based on different factors.

As the debate over the scope of consumer welfare rages on, this proposal offers some shared understanding at the interface of antitrust law and data privacy. It can be adopted alongside either the separatist or integrationist viewpoints. Regardless of which view is taken in liability-stage analysis, consideration of data privacy makes sense in the design of remedies.

It is only fair to acknowledge the potential challenge inherent in this proposal: it requires consideration of potential tradeoffs between the privacy harms and the competition expected to be restored by the remedy. Weighing such harms against each other with precision may well prove difficult.[239] This is particularly true because data privacy law is at an early stage of defining the legally cognizable harms that arise from privacy incursions.[240] But even if this balance is not determinable with "Euclidian precision," it is worthy of consideration.[241] The improvement of consumer welfare, which lies at the heart of antitrust enforcement, may well be at stake. This is a compelling reason to consider data privacy in the design of remedies.

Finally, it is worth noting that in the design of antitrust remedies past, remedial orders have accommodated factors

---

[239] *See, e.g.*, on the liability-stage analysis challenges, Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON., May 2014, at 5-6 (analysis of data privacy and competition tradeoffs in product design is likely to be challenging because a reduction in privacy often leads to improvement of some other product quality or attribute, and the magnitude of the privacy harm is difficult to assess).

[240] *See, e.g.*, In re Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *5-10 (N.D. Cal. Dec. 3, 2013) (discussing various unsettled theories of injury-in-fact to privacy for the purposes of determining Article III standing).

[241] Thomas B. Leary, *Competition Law and Consumer Protection. Law: Two Wings of the Same House*, 72 ANTITRUST L.J. 1147, 1148 (2005) (potential ambiguity in determining the tradeoff between consumer protection and competition does not obviate the need for this analysis).

similar to privacy. The settlement in *Microsoft* included exceptions to the defendant's disclosure obligations for data security. Microsoft was not required to provide APIs or other information where such disclosure would compromise the security of its anti-virus or other security systems.[242] In fact, when several non-settling states sought more extensive and earlier disclosure of Microsoft's API data, the D.C. Circuit refused on grounds of data security.[243] The court found that pushing the API disclosure to earlier would likely reduce data security, which in turn was likely to cause consumer harm.[244] An exclusion on data security grounds was also included in a 2005 remedy the DOJ obtained against the National Association of Realtors. Home listing data related to "security of the listed property" could be withheld from disclosure under the order, provided that the data was withheld equally from both traditional and online realtors.[245] Like data security, data privacy is a reasonable factor to consider and accommodate in order to avoid collateral harm from the imposition of a remedy.

A. Implementing the Proposal

In implementing this proposal, courts and agencies will first need to consider whether the anticipated remedy implicates the disclosure, access, collection, sale or other use of consumer information. If so, then their analysis should consider whether and how any reasonable expectations of privacy held by consumers are implicated by the expected remedial order. Though case specific, this assessment might consider factors like the type of data subject to the remedy, the uses of the data

---

[242] United States v. Microsoft, No. 98-1232 (CKK), 2009 WL 1348218, at *6 (D.D.C. Apr. 22, 2009) (originally entered Nov. 12, 2002; modified Sept. 7, 2006; further modified Apr.22, 2009).

[243] Massachusetts v. Microsoft Corp., 373 F.3d 1199, 1221–22 (D.C. Cir. 2004) (affirming the district court's refusal to expand API disclosure, based on concern that broader or earlier API disclosure obligations could force Microsoft to publish APIs that were not yet sufficiently stable or secure, and could also negatively impact Microsoft's incentives to innovate).

[244] *Id.* at 1219 (affirming District Court denial of an expanded disclosure remedy as "likely to harm consumers").

[245] *See* United States v. Nat'l Ass'n of Realtors, 2008 WL 5411637, at *13 (N.D. Ill. Nov. 18, 2008) (allowing listing data to be withheld regarding "showing or security of the listed property").

that will be permitted by the remedial order, whether the data is being sold and which entities will be permitted to have access to the data.

Where a remedy implicates reasonable expectations of privacy, courts and agencies will then need to consider the tradeoff between protecting those expectations and restoring data-driven competition. The question will become whether the antitrust remedy should be modified to account for those privacy interests. If so, how and to what extent should the remedy be changed to protect consumer data privacy? For example, the agency or court could impose obligations or limits on the competitors' use of consumer data, or require certain protection of the data after it is received.[246]

The data privacy implications of the remedy may be evident from the nature of the misconduct. However, there are at least two scenarios in which remedies may impact privacy even when the anti-competitive conduct does not. Antitrust courts and enforcers should be particularly alert to privacy impacts in these situations, where the current, liability-focused theories are likely to miss the data privacy impacts caused by remedies.

The first type of scenario is illustrated by the Google example at the outset of this article, in which Google terminates a rival's API access in an anti-competitive manner. Google's conduct was anti-competitive, but it was also privacy-enhancing, because it limited access to private consumer information.[247] The remedy reversed the misconduct, and so resulted in greater access to and use of user information. The

[246] In at least one past merger remedy, the rivals who received company data went on to abuse it by using the data beyond the limits of the compulsory license. Following the settlement in *Nielsen Holdings N.V. and Arbitron Inc.*, File No. 131 0058 (Sept. 20, 2013), Nielsen sued the recipient of its demographic data, provided pursuant to an antitrust order for compulsory data licensing. *See* Complaint, No. C-4439 (F.T.C. Feb. 28, 2014), https://www.ftc.gov/system/files/documents/cases/140228nielsenholdingscmpt.pdf.

[247] *See supra* Section II.C. *Existing Theories on Antitrust Law /Data Privacy Interface Do Not Address Remedies*.

effect of the remedy in such a situation is to erode data privacy, in favor of improving data-driven competition. Courts and agencies should consider data privacy in the design of the remedies when this occurs.

Second, impacts on privacy may arise only at the remedies stage of a case when the remedy is broader in scope than mere termination of the misconduct. It is "well-settled law" that the scope of antitrust equitable relief may go beyond the prohibition of the practices found unlawful.[248] The Supreme Court explains that relief under the Sherman Act is "not limited to the restoration of the *status quo ante.*"[249] It is not uncommon for the remedy to be at a higher level of abstraction than the misconduct, because a reversal of the misconduct may be insufficient to achieve the antitrust remedial goals of restoring competition and preventing future violations.[250]

Microsoft provides an example of this type of asymmetry between the misconduct and the data access remedy. The company's violations of the Sherman Act did not involve denying rivals access to APIs or server protocols, yet the remedy

[248] *See* Trabert & Hoeffer, Inc. v. Piaget Watch Corp., 633 F.2d 477, 485 (7th Cir. 1980) (stating that "settled" law establishes that for relief to be effective, it may go beyond the "narrow limits of the proven violation" of the Sherman Act); Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 697–98 (1978) ("When the purpose to restrain trade appears from a clear violation of the law, it is not necessary that all of the untraveled roads to that end be left open and that only the worn one be closed."); PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW: AN ANALYSIS OF ANTITRUST PRINCIPLES AND THEIR APPLICATION ¶325c (4th ed. 2020) ("The decree may also contemplate and forbid conduct that is different from the conduct that was actually condemned. Indeed, the court may even prohibit lawful conduct if such a prohibition 'represents a reasonable method of eliminating the consequences of illegal conduct.'" (quoting Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 698 (1978)); Melamed *supra* note 17, at 363–64 (discussing the challenge in determining the "appropriate level of abstraction or generality for a remedy" that seeks to prevent recurrence of anti-competitive conduct).

[249] Ford Motor Co. v. United States, 405 U.S. 562, 573 n.8 (1972).

[250] *Ford Motor Co.*, 405 U.S. at 573 n.8 (1972); Associated Press v. United States, 326 U.S. 1, 22 (1945) (holding that trial court is empowered to craft an antitrust remedy that prevents future violations).

required Microsoft to disclose that information to rivals.[251] The remedy went beyond simply ending the misconduct to "prevent recurrence of similar conduct in the future and restore competition in the software market."[252]

The implication of such asymmetry is that even if the anti-competitive conduct does not implicate data privacy, the remedy may. An antitrust remedy could grant access to private data or override privacy settings as part of the action required to restore competition or prevent future misconduct. When the consent decree or other remedy goes beyond a reversal of the misconduct to require such processing of data, it may implicate consumer data privacy. The privacy impacts are a collateral or side effect of the desired antitrust remedy, and ought to be considered by the court or agency.[253]

1. Short-Term Reconciliation: Consent-to-Remedy

So far, this article has largely left aside the implications of notice and consent on the design of data access remedies. Under a notice and consent model of data privacy protection, companies provide a description or "notice" to consumers disclosing how their data will be collected, used, shared or sold. The consumer can then choose whether or not to consent to the activities described.

The FTC and companies have long used notice and consent to confer consumer control over personal data. As Barocas and Nissenbaum explain, "informed consent is a natural corollary of the idea that privacy means control over information

---

[251] Renata B. Hesse, *Section 2 Remedies and U.S. v. Microsoft: What Is to Be Learned?*, 75 ANTITRUST L.J. 847, 859 (2009) (observing the data disclosure obligations imposed on Microsoft did not relate directly to liability findings).

[252] *DOJ Microsoft Settlement Press Release*, *supra* note 110.

[253] William E. Kovacic, *Designing Antitrust Remedies for Dominant Firm Misconduct*, 31 CONN. L. REV. 1285, 1310 (1999) (observing that a court should "identify possible side effects from implementing the contemplated remedy").

about oneself." [254] Where sufficient notice and consent is obtained, the FTC has historically viewed privacy as being adequately protected. Provided that the data is collected and used within the parameters of the consumer's notice and consent, there was thought to be no data privacy harm.

This suggests data access remedies could adopt a "consent-to-remedy" model to reduce potential harm to privacy arising from remedial disclosures of information. As part of the remedy, consumers could be provided with notice describing how their data will be disclosed and used under the remedy, and then their consent could be sought for that data processing. The remedial order would then provide an exception to the defendant's obligations to grant data access, carving out any data of consumers who refused to consent. Consumers would choose for themselves whether data privacy or data competition is more beneficial. If harm to consumers occurs only when their private information is used, collected or sold without sufficient notice and consent, then designing and implementing the antitrust remedy contingent on consumer consent should eliminate such harm.

The DOJ's 2005 case against the National Association of Realtors offers an early-stage glimpse into this consent-to-remedy approach. The DOJ challenged the Association's new member policy as a violation of Section 1 of the Sherman Act.[255] The policy empowered the Association's member realtors to deny online competitors access to listings of homes for sale. Though it seems dated now, the traditional model for home sales was that only realtors could directly access the listings of properties available for sale. Real estate brokers would provide selected listings to clients via email, fax, mail or even hand delivery. New entrants began to introduce online business

[254] Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44, 57 (Julia Lane et al. eds., 2014).

[255] Amended Complaint at 13, United States v. Nat'l Ass'n of Realtors, No. 05-C-5140, 2008 WL 5411637 (N.D. Ill. Nov. 27, 2006), https://www.justice.gov/atr/case-document/amended-complaint-6. Though this case was under Section 1 of the Sherman Act rather than Section 2 (the focus of the discussion here) the remedies are instructive in their implications for privacy and data access.

models wherein they allowed consumers direct, electronic access to for-sale listings. These new realtors charged lower commission rates than traditional realtors, creating price competition. In response, the Association tried to shut out these new entrants by limiting their access to home listings data. The Association's new policies empowered traditional realtors to withhold their "for sale" home listings from the same online competitors who were undercutting realtor prices.[256]

The remedy in the case required the Association to change its policy to make property listing data available to online realtors on the same terms as traditional realtors. Importantly here, the remedial order also provided that consumers could opt-out of having their home listing data displayed online by completing a "seller opt-out form."[257] The form empowered the consumer to withhold their listing from online realtors, or to exert certain other controls if they permitted the listing to be online, such as prohibiting the display of an automated estimate of the market value of their home in the online listing.[258] Consumers sensitive to having the details of their homes spread online for all to see could thus withhold their listing information from online realtors. In essence, the remedy assumed consumer consent to inclusion of home listing data in the remedy unless the consumer opted out. The neutral treatment obligation in the remedy did not apply when consumers opted out, and so Association members were free to withhold those "opt-out" listings from online realtors.

The problem hinted at by this early consent-to-remedy approach is the tradeoff it creates between the different goals of a well-designed antitrust remedy. Recall that a remedy seeks to avoid unintended harm, to be effective in achieving its remedial objectives and to be administrable by the supervising court or

---

[256] The Association policy required its member organizations to forbid any realtor from granting their customers direct access to listings, unless the listing agent granted his or her permission. It was generally traditional realtors who listed properties for sale, so this enabled traditional agents to withhold their listing information from new entrants. *Id*. at 3.

[257] United States v. Nat'l Ass'n of Realtors, No. 05-C-05140, 2008 WL 5411637 at Exhibit A, ¶ II.5(a) and (b) and Appendix A "Seller Opt-Out Form" (N.D. Ill. Nov. 18, 2008).

[258] *Id.* at Exhibit A, para II.5(c).

agency. Requiring consumer consent to remedial data disclosure may reduce unintended privacy harm to consumers, but this is likely to come at the cost of reduced effectiveness in restoring competition and reduced administrability of the remedy.

A consent requirement threatens to undermine the effectiveness of the remedy by placing its success in the hands of individual consumers. The premise of a data access remedy is that rivals need to obtain access to the information to restore competition. Making that access contingent on consumer consent gives those consumers the power to threaten the implementation of the remedy. If individuals refuse consent, the exercise of their data privacy interests prevents the remedial data transfer.

In a worst-case scenario, a large number of consumers could opt-out of permitting their data to be shared under the remedy (or refuse to opt-in, a more likely approach under current data privacy standards). This could prevent the implementation of the remedy at a scale that enables restoration of competition, undercutting its effectiveness. A consent-to-remedy approach prioritizes consumer privacy interests over the fulsome implementation of the data access remedy, and by doing so, leaves the effectiveness of the remedy in the hands of those consumers.

This difficulty relates back to the conception of data privacy as consumer control. When consumers are granted control over the use of their data, that means consumers can protect their privacy interests, but it also means they can control whether the remedy is implemented. Although privacy control over data is not absolute,[259] there have not yet been any exceptions to that control articulated for antitrust remedies.

Even in a best-case scenario where consumers consent in sufficient proportion to implement an effective remedy, a consent-to-remedy approach adds administrability costs for

[259] WESTIN, *supra* note 213, at 46 (contemplating exceptions to data privacy "in the interests of society," but calling them "only extraordinary"). Notice and consent is itself an example of the non-absolute nature of privacy control. When granted, data can be used in accordance with that consent.

supervising courts, agencies, and defendants. Seeking consent to the transfer and use of data (particularly if every consumer is required to opt-in), accommodating consumers who decline consent or who express variations on their consent, and policing later data misuse adds time and costs to the implementation, supervision and enforcement of the remedial order. Even in the National Association of Realtors case involving relatively simple property listing data, the optionality for consent and enforcement mechanisms multiplied quickly.[260] These administrability challenges may well grow in cases with higher volume, more complex data-driven businesses—like digital platforms. The consent-to-remedy approach thus offers a tradeoff between protecting data privacy of consumers and achieving effective and administrable data access remedies.

Even if consent-to-remedy offers a workable short-term solution for reconciliation of data access remedies with privacy, there are long term challenges on the horizon. The tradeoffs between privacy protection and remedial effectiveness will only grow as data privacy interests expand.

Though notice and consent remains the most common mechanism for conferring consumer data privacy, it is roundly criticized for its narrowness and inadequacy—including by the FTC itself.[261] The volume and complexity of privacy policies that consumers are exposed to online have rendered notice and

---

[260] Consumer opt-outs in the National Association of Realtors case required completion of a form by each individual home seller that included different data-related options. Those options would then have to be implemented in data access permissions, and the Association also had to retain the form for a set period of time as evidence of opt-out. Realtors were required to have browsing buyers who accessed the online listing data agree to use the data only for the purposes indicated in the remedial order. United States v. Nat'l Ass'n of Realtors, No. 05-C-5140, 2008 WL 5411637, at *8 (N.D. Ill. Nov. 18, 2008) (limiting potential buyers who access online listings from use of that data for anything other than "personal, non-commercial" purposes, and requiring certification of their "bona fide interest in the purchase, sale or lease" of the offered real estate).

[261] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable, at 3 (Dec. 7, 2009) (acknowledging that "consumers don't read privacy policies"). For further criticism of the notice and consent approach, *see generally*, Pasquale, *supra* note 4; Slaughter, *supra* note 230.

consent largely a legal fiction. Consumers could never realistically read, much less understand, the myriad of disclosures governing the collection and use of their data.[262] Even if consumers do read privacy notices, they often have little meaningful choice but to accept the terms as presented by companies.[263] Notice and consent has become a way to exploit the rational ignorance of consumers, a mechanism that is more likely to protect the company seeking consent than the consumer giving it.[264] In 2019, one FTC Commissioner declared "it is time for the reign of notice and consent to end."[265]

Current approaches to notice and consent reflect a thin conception of privacy interests. The accommodation within antitrust can be correspondingly thin, as with a consent-to-remedy approach. The notice and consent model permits reconciliation with antitrust remedies by virtue of its minimalist view of data privacy interests. Though critical of both legal approaches, Frank Pasquale observes this current match between the short-term orientation of antitrust and data privacy law: "The narrowness of 'notice-and-consent' as a privacy model nicely matches the short-term economic models now dominating American antitrust law."[266] This match enables a largely mechanical reconciliation of data privacy and antitrust through approaches like consent-to-remedy, instead of demanding a more substantive or principles based theory of interaction between these areas of law.

---

[262] An oft-cited 2012 article estimated that it would take a consumer 76 days to read the privacy policies encountered in the span of just one year. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012) https://www.theatlantic.com/technology/archive/2012/03/reading-theprivacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851. One can imagine the figure would be much higher now, given the growth in online activity of consumers since 2012.

[263] Slaughter, *supra* note 230 (noting almost no power of consumers to negotiate privacy terms and potentially few alternative services available).

[264] Pasquale, *supra* note 4, at 1012 ("Consumers neither experience nor hope for meaningful protection of privacy in the 'terms of service' foisted on them and the 'privacy settings' that leading companies offer them.").

[265] Slaughter, *supra* note 230.

[266] Pasquale, *supra* note 4, at 1010.

However, all indications are that the U.S. is moving toward more robust conceptions of data privacy interests. Scholarly and political voices regularly press for omnibus federal privacy legislation, as does the FTC.[267] There is widespread support for such legislation, and a number of bills have been introduced.[268] In the meantime, states are taking the lead in expansive rights-based data privacy legislation, as well as sectoral laws on matters like facial recognition and mobile application data protection.[269] Even without new federal privacy legislation, the FTC has expanded data privacy protection from its earlier privacy "promises" enforcement model to more robust protection of consumers' reasonable expectations of privacy, independent of company representations.[270] This shift has been described as "profound," because it hints at the beginning of a much more substantive and complete protection of data privacy in the U.S.[271] Further, the information considered "personally identifiable" and thus often protected, is expanding. As digital data proliferates, it is becoming apparent that this creates greater potential for cross-identification and de-anonymization of many

---

[267] *See, e.g.*, Issie Lapowsky, *Get Ready for a Privacy Law Showdown in 2019*, WIRED (Dec. 27, 2018) (summarizing the myriad of proposed bills on federal privacy law from industry, Senators and federal agencies); Council on Foreign Relations, *Reforming the U.S. Approach to Data Privacy* (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (calling on Congress to pass comprehensive federal privacy legislation); FTC PROTECTING CONSUMER PRIVACY REPORT, *supra* note 209, at i ("[I]t is time for Congress to enact baseline privacy legislation").

[268] *See, e.g.*, Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) and the House companion Bill, Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019).

[269] *See, e.g.*, California Consumer Privacy Act of 2018 Cal. Civ. Code § 1798.100–1798.199 (2018); Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15 (West 2018) (establishing privacy protection of biometric information); Delaware Online Privacy and Protection Act, DEL CODE ANN. TIT. 6 §§ 1201C-1206C (2015) (establishing data privacy protection related to mobile applications).

[270] *See* discussion *supra* Section III.B.1. *The Rise of Data Privacy Law and its Application to Digital Platforms*; Solove & Hartzog, *supra* note 72, at 662 (describing the shift from a privacy promise enforcement model to substantive standards).

[271] Solove & Hartzog, *supra* note 72, at 666.

types of information.[272] Each of these developments signals the growing scope of data privacy protection in U.S. law.

As U.S. law moves toward more robust protection of data privacy, antitrust will be harder pressed to accommodate privacy interests within effective antitrust remedies. The stronger and broader data privacy interests become, the more acute the tradeoffs are likely to be if antitrust remedies except those interests. This trend is already evident in reflection on the 2005 National Association of Realtors case. That remedy offered consumers only the option to opt-out of sharing their data. Now the FTC strongly prefers opt-*in* default settings for public data disclosure, meaning consumers affirmatively chose to share their information.[273] This is the difference between consumers bearing the obligation to prevent such sharing, as in the Realtor case, and the company bearing the burden of obtaining consent for data sharing.

The difference between opt-out and opt-in is more significant than it seems, because consumers tend to accept default settings. In the National Association of Realtors remedy, that meant data sharing was likely to occur. If consumers are now required to opt-in to a remedy, rather than opt-out, that lowers the likelihood of sufficient consumer participation in data sharing for an effective antitrust remedy. Less data is likely to be disclosable. This difference could also increase the administrative burden of the remedy on defendants, courts and agencies, from managing rarer opt-outs to ensuring that affirmative consent is obtained for all of the data that is accessed by rivals.

The greater the scope of data privacy accommodation required within the remedy, the more acute the tradeoff becomes with administrability and effectiveness. As privacy interests strengthen, accommodation of those interests within data access remedies will grow to be a larger and larger. Eventually, that accommodation may threaten the remedy entirely, rendering

---

[272] Gindin, *supra* note 208; REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE *supra* note 208.

[273] Solove & Hartzog, *supra* note 72 at 661 (discussing FTC preference for opt-in settings).

impossible or impracticable the data access that the remedy seeks to provide as a means of restoring competition. Consent-to-remedy is thus a starting point, not a lasting answer to the larger normative questions at the intersection between data privacy and data competition.

2. Long-Term Reconciliation: Defining Data Privacy Interests to Exclude Remedial Data Processing

As courts, agencies and legislators are increasingly pressed to decide between data privacy and competition remedies, a second possible approach is to define the scope of data privacy interests to exclude lawful disclosure of data pursuant to a remedy. In other words, there would be no tradeoff in the eyes of the law, because the legally cognizable data privacy interests of individuals do not extend to the disclosure ordered by an antitrust remedy. Though the effects on consumers from disclosure of private data may look similar, whether ordered by a remedy or otherwise, this treats the legal order itself as the distinguishing factor.

Data privacy interests are new, and the edges are fuzzy and evolving. It is not beyond contemplation that, as those interests crystalize in U.S. law, the disclosure of data pursuant to a court order is found to be outside of recognized consumer data privacy interests. Since any tension between data privacy and antitrust law depends on the scope of each, this reconciliation leaves it to data privacy law to delineate its boundary as non-overlapping with antitrust remedial orders.

The European Union's General Data Protection Regulation ("GDPR") provides an example of this approach. The GDPR expressly excepts processing of personal data from data privacy rights when such processing is "necessary for compliance with a legal obligation" imposed on the company controlling the user data.[274] Though this legislative wording is not specific to antitrust remedial orders, some scholars argue that court-ordered antitrust remedies are likely to be considered such

[274] Commission Regulation 2016/679, art. 6(1)(c), 2016 O.J. (L 119) 1, 36.

a "legal obligation."[275] If this exception applies, a defendant could process user data as required by the remedial order without violating user data privacy rights. This approach resolves the potential legal conflict where an antitrust remedy imposes obligations to disclose data in the face of data privacy obligations that prohibit such processing.[276] It does so by creating an exception or safe harbor from the application of data privacy law for antitrust remedial data processing.

The new California Consumer Privacy Act contains a more general exception that could be read similarly to the GDPR provision. The California legislation provides that "[t]he [privacy protection] obligations imposed on businesses by this title shall not restrict a business's ability to…comply with federal, state, or local laws."[277] The language in the California Act is not as clear as that in GDPR, but it could be interpreted

---

[275] *See, e.g.*, Inge Graef *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Alphen aan den Rijn, Kluwer (2016) at 312 (arguing that the GDPR exception to permit data processing for "compliance with a legal obligation" would be a legitimate basis for data processing pursuant to an antitrust remedial order) *but see* V. Kathuria & J. Globocnik, Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy, Max Planck Institute for Innovation and Competition Research Paper No. 19-04, 2019, https://ssrn.com/abstract=3337524 (arguing that the same GDPR exception does not apply to permit data processing required by antitrust remedies, because the exception requires an obligation under a "generally applicable" law, rather than a specific case judgement or order).

[276] This exception is required to avoid such conflict in the EU because EU data privacy law takes the opposite default position on data processing as U.S. law. In the EU, the processing of personal information is *not* permitted absent a legal basis, meaning that without an applicable exception, the processing of data under an antitrust remedy would violate EU data privacy law. It is only because the U.S. takes the opposite default position—that data process is permitted unless stated otherwise—that there is no hard conflict at present in U.S. law between an obligation to disclose data and an obligation to protect it. There is instead the softer policy question addressed here of whether and when to prefer data privacy or data competition at the margins of a remedy. Schwartz & Solove, *supra* note 177 (observing the opposite in default position on data privacy protection in U.S. and European law).

[277] The California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.145 (a)(1) (2018).

similarly, as an exception from data privacy rights for antitrust remedial orders made pursuant to the listed laws.

There is no equivalent exclusion at the federal level, because the U.S. has no omnibus federal privacy legislation. However, as the U.S. moves toward enactment of an omnibus federal data privacy statute, legislators should consider whether to include such an exception from privacy rights. The exception for orders that would otherwise conflict with data privacy law is not only an issue for antitrust remedies, but for other laws or orders that require disclosure of private data. In the continuing absence of omnibus federal legislation, courts and antitrust agencies could also articulate a similar view, drawing boundaries around their definitions of data privacy interests to exclude disclosure and use of personal data pursuant to a lawful order.

Both the advantage and disadvantage of this exclusion approach lie in its simplicity. It systematically prefers competition remedies to data privacy protection at the margin where the two meet. This offers easier reconciliation for courts and agencies between data privacy and antitrust remedies. It obviates the need to address case-by-case questions about when, whether and to what extent data access remedies should be modified to account for user data privacy. As the consent-to-remedy approach shows, these questions can multiply quickly and may prove difficult to answer. This exclusion approach resolves the potentially challenging task of weighing the privacy harms of remedy against the data-driven competition benefits.

However, defining data privacy rights to exclude remedial disclosure also creates a standing assumption that data-driven competition should be preferred over data privacy at this intersection. It implies that whatever harms to data privacy arise from the antitrust remedy, the law has considered and accepted them in the interest of restoring competition and ensuring compliance with legal orders.

It is not yet clear that this systematic preferencing of competition is the best approach for consumers in every case. As this article shows, we are only beginning to understand the intersection of data privacy and data competition, particularly

with regard to remedies. Though it seems doubtful at this juncture, it may even be that the GDPR has this preference the wrong way around—perhaps antitrust law should systematically except private data from disclosure in an antitrust remedy. These different options, and the tradeoffs they entail, deserve reasoned consideration that has yet to occur. Until it does, it seems premature to systematically prefer remedies. This exclusion approach is best thought of as a longer-term possibility. In the interim, the case-by-case analysis should help to inform a stronger theoretical understanding of the tradeoffs between data privacy and data access remedies.

V. CONCLUSION

Antitrust agencies are on the verge of landmark monopolization cases against digital platforms. The remedies in such cases will demand new and careful consideration of data privacy.

Monopolization remedies in cases past did not generally involve consumer data. Those that did largely predate the rise of U.S. data privacy law. Historical data access remedies therefore had no cause to contemplate consumer privacy interests in the information subject to disclosure.

That is no longer the world in which antitrust remedies live. Consumer data has become a major driver of digital commerce. The rise of data privacy law has brought about new protections and consumer control over large swathes of that data. For the first time, data access remedies may well implicate *our* private information.

Existing theories on the intersection of antitrust law with data privacy stop short of addressing these developments. Their focus is on analysis of liability. As this article explains, even if data privacy is not impacted at the liability stage of a case, it will be impacted by a remedy that requires access to private information to restore competition.

This article calls for antitrust analysis to consider data privacy in the design of remedies, particularly for digital platforms. If data privacy is ignored, the risk is a remedy that

causes privacy harms that outweigh the benefits to consumers from restoration of data-driven competition. Such a remedy would reduce overall consumer welfare, and therefore defeat the goal of bringing antitrust enforcement action.

The article describes two potential approaches to update antitrust thinking on remedies and data privacy. Short term, courts and agencies could seek consumer consent to the disclosure and use of private data pursuant to a remedy. However, this "consent-to-remedy" approach may not stand the test of time. It presents growing tradeoffs between data privacy protection and the design of effective and administrable antitrust remedies. A second, longer term option is for legislators or courts to define data privacy interests as excluding the disclosure or use of data when ordered by an antitrust remedy. However implemented, now is the time to deepen our understanding of how data privacy impacts monopolization remedies—before jumping ahead to such remedies against digital platforms.