The Antitrust and Privacy Interface: Lessons for Regulators from the Data*

Brijesh Pinto,† D. Daniel Sokol‡ & Feng Zhu§

Abstract. This Article will review empirical evidence on the effects of privacy laws—particularly those regulating personal data collection and use—on competition, aiming to inform regulators regarding potential antitrust impacts. Regulators often assume that competition laws cannot sufficiently address antitrust issues in digital services markets and may view privacy regulations as a means to bridge antitrust gaps to foster competition, viewing them as generally pro-competitive. However, empirical evidence reveals a more complex relationship between privacy regulations and competition, indicating that through their impacts on market concentration, firm entry and exit, advertising, contracting, and compliance costs, among others, privacy laws can potentially undermine competition and even erode consumer privacy. Informed by the empirical evidence, privacy and antitrust regulators should account for these effects in crafting and deploying regulations.

* The authors thank Megan Aved and Richard Xu for their excellent research assistance. Sokol and Zhu have provided consulting services to Alphabet and Meta. They have done consulting work specifically on the topic of competition and privacy. The authors significantly revised and expanded this Article based on Sokol and Zhu's prior work, "Harming Competition and Consumers Under the Guise of Protecting Privacy: Review of Empirical Evidence," (which received support from Meta Platforms, Inc.) published by Competition Policy International in December 2022: https://perma.cc/TE6S-BZ5B.

† Associate Professor of the Practice of Economics, University of Southern California.

‡ Carolyn Craig Franklin Chair in Law and Professor of Law and Business, University of Southern California Gould School of Law and Marshall School of Business; Senior Advisor, White & Case LLP.

§ MBA Class of 1958 Professor of Business Administration at Harvard Business School.

Introduction

On May 25, 2018, the General Data Protection Regulation ("GDPR")[1] came into force in the EU, and approximately one month later, the California Consumer Privacy Act ("CCPA") was enacted in the United States.[2] These two landmark privacy acts, which bore upon firm conduct and market outcomes, sparked policy debates regarding the interactions between privacy laws and antitrust regulations.[3] For example, in the same year, a series of hearings at the U.S. Federal Trade Commission ("FTC") explored the analytical significance of personal data in matters of competition and innovation.[4] Among the issues discussed was whether "the presence of personal information or privacy concerns inform or change competition analysis."[5] Antitrust agencies worldwide have increasingly focused on the interface of competition and privacy, as have courts and academic scholarship.[6]

As a prefacing observation, sound antitrust policy design and enforcement can, under certain parameters, positively affect privacy protection independent of digital privacy regulations. If customers care about privacy, firms may compete along this non-price dimension. In this case, Pamela Harbour and Tara Koslov noted that platforms' privacy policies essentially serve as a strategic variable; firms respond to changes in competitors' policies.[7] Similarly, in its review of Microsoft's acquisition

---

[1] Council Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 87 (EU) [hereinafter GDPR].

[2] Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 71–72 (2018).

[3] *See, e.g.*, *FTC Hearing #6: Privacy, Big Data, and Competition*, FED. TRADE COMM'N, https://perma.cc/ZQ5J-U65L.

[4] *Id.*

[5] *Id.*

[6] *See* Epic Games, Inc. v. Apple Inc., 559 F. Supp. 3d 898, 1042–43 (N.D. Cal. 2021), *aff'd in part, rev'd in part*, 67 F.4th 946 (9th Cir. 2023); Press Release, Fed. Trade Comm'n, FTC Announces September 22 Workshop on Data Portability (Mar. 31, 2020), https://perma.cc/QBA4-PH43 (noting that data portability rights provided by privacy laws may promote competition); Joaquín Almunia, Vice President, Eur. Comm'n for Competition Pol'y, Speech at the European Commission Privacy Platform Event: Competition and Personal Data Protection (Nov. 26, 2012), https://perma.cc/2KCT-PKPQ; Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. F. 647, 649 (2021); Alexander Bleier, Avi Goldfarb & Catherine Tucker, *Consumer Privacy and the Future of Data-Based Innovation and Marketing*, 37 INT'L J. RSCH. MKTG. 466, 470, 475 (2020).

[7] 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, 793–94 (2010) ("As demonstrated by recent studies, online privacy is an important issue for many consumers, especially with regard to targeted behavioral advertising. Moreover, consumer awareness of privacy issues continues to grow, driven in large part by enforcers' increased scrutiny and consumer education efforts, which have led firms to improve transparency regarding their privacy policies. Apparently, the online firms are listening—many of the

of LinkedIn in 2016, the European Commission ("EC") noted that "[p]rivacy-related concerns . . . do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor."[8]

Regardless, policymakers have increasingly turned their attention to the antitrust role of data privacy regulations against the backdrop of widespread digital transformation.[9] To ensure policy is not founded on unrealistic assumptions, a deeper understanding of the intersection between privacy laws and competition will play an important role in guiding the design and assessment of regulations and policy choices.[10] Evidence regarding the impact of privacy laws on competition is still forthcoming—for example, in 2019, Alessandro Acquisti remarked it would "take probably a few years . . . before the dust settles and a clear picture of the economic impact of GDPR can emerge."[11] This Article reviews the expanding collection of empirical evidence with this proviso

---

biggest Internet names publicize their privacy policies as a way to attract and retain users. Even more importantly, these firms react directly to each other's privacy policy changes. At one point in 2008, Google, Yahoo!, and Microsoft each shortened the amount of time they would retain personal data gathered from users' Web surfing. Interestingly, Microsoft announced that it would anonymize its data after six months—compared to the firm's then-existing eighteen-month policy—but only if its rivals would follow suit. Yahoo! subsequently announced that it would retain data for only three months, albeit according to a different anonymization standard. And one industry commentator noted that first-mover Google had 'started this competition,' putting other firms in a position where they needed to respond.") (footnotes omitted). *But see* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right *[Approach]* to Privacy, 80 ANTITRUST L.J. 121, 138 (2015) (suggesting complementary roles for privacy and competition).

[8] European Commission Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://perma.cc/2FVE-QCJA. The Commission further remarked: "In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction." *Id.* Still, there is a gap between identifying and analyzing a non-price dimension for antitrust purposes. *See, e.g.*, Allen P. Grunes, *Another Look at Privacy*, 20 GEO. MASON L. REV. 1107 (2013). Reflecting on the U.S. experience up to 2012, Grunes argued that

> [f]irms do compete on privacy protection; think, for example, of Microsoft's advertising campaign aimed at Safari users after Google got caught bypassing Safari's privacy settings. . . . But this dimension of competition is not very widespread or intense today. One would look in vain for any DOJ or [FTC] cases that speak of a "loss of privacy competition" as a competitive effect. And there are reasons to doubt that privacy will ever reach the status of price, quality, or innovation in an antitrust review.

Id. at 1112 (footnote omitted).

[9] *See FTC Hearing #6*, *supra* note 3.

[10] *Id.*

[11] Alessandro Acquisti, Privacy, Economics, and Regulation: A Note 18–19 (May 2019) (unpublished manuscript) (on file with author).

in mind.[12] This Article also sheds light on the privacy and antitrust interface by providing an overview of the current empirical evidence on the intersection between privacy laws—chiefly, the GDPR in the EU and the CCPA in the United States—on antitrust issues as well as papers that address this interaction through private governance via contracting.

In summary, privacy laws and regulations are complex assortments of conditions that can impact competition at different points and in different ways; for researchers, privacy regulations such as the GDPR and CCPA provide a natural experiment to study myriad effects, including competitive impacts. As illustrated by the following literature review, empirical analyses generally reveal that the impacts of privacy laws on competition depend on the specific business facts and economic forces in play, and under certain circumstances these regulations may negatively impact competition. Our exploration of the evidence serves to caution regulators that sweeping privacy regulations can give rise to unintended consequences for both competition and privacy.

I. Privacy, Competition, and Welfare: An Overview

Though privacy itself is challenging to define and measure, recent regulations have focused on safeguards relating to personal data, such as the EU's GDPR, which "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[13] Similarly, in the United States, the CCPA "gives consumers more control over the personal information that businesses collect about them."[14] Thus, privacy regulations such as the GDPR and the CCPA directly impact firm conduct, thereby influencing firms' ability to compete—particularly in digital industries—and potentially distorting market outcomes.

Such privacy regulations seem to address increasing consumer awareness of online privacy issues—largely driven by heightened scrutiny from regulatory bodies, including several high-profile cases related to data privacy—and widespread consumer concern regarding targeted behavioral advertising.[15] The growing public awareness and concern, compounded by regulatory pressure, have prompted firms to pay greater

---

12 To be sure, this Article addresses recent regulatory and marketplace developments, and certain empirical studies are working papers still under review.

13 GDPR, *supra* note 1, at 32.

14 *California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST., https://perma.cc/BB9B-HHM6 (last updated Mar. 13, 2024).

15 *See* Russell Heimlich, *Internet Users Don't Like Targeted Ads*, PEW RSCH. CTR. (Mar. 13, 2012), https://perma.cc/GJV8-PCWB; *see also* Hyejin Kim & Jisu Huh, *Perceived Relevance and Privacy Concern Regarding Online Behavioral Advertising (OBA) and Their Role in Consumer Responses*, 38 J. CURRENT ISSUES & RSCH. ADVERT. 92, 94–96 (2017).

attention to consumers' data protections and amend their privacy policies in relation to how they collect, use, and protect consumer data.[16]

All else equal, because consumers regularly affirm their privacy concerns in surveys, it may appear that the enhanced data-flow protections would increase consumer welfare.[17] However, the reality is far from *ceteris paribus*. Beyond protections relating to users' personal information, consumer welfare is also a function of price, quality, variety, and other aspects of the products and services they purchase or use online—all of which are fashioned by competitive forces and impacted by the laws that regulate firm conduct, including privacy laws.[18] The empirical record reflects this reality: privacy-protection policies can entail substantial costs in foregone innovation and lead to higher prices and decreased product variety or quality, suggesting that privacy laws do not necessarily increase overall consumer welfare.[19]

For example, Samuel Goldberg et al. offered quantitative insight into how privacy laws may have a positive first-order effect on consumer

---

16 *See* FED. TRADE COMM'N, THE FEDERAL TRADE COMMISSION 2023 PRIVACY AND DATA SECURITY UPDATE 3–4 (2023), https://perma.cc/X4UQ-P2Y6 ("Beyond case-by-case enforcement, the FTC also develops, amends, and enforces various rules related to privacy and data security, and works to educate both businesses and consumers about privacy and data security issues."); *see also Privacy*, APPLE, https://perma.cc/V7EX-5N53; CISCO, 2023 CONSUMER PRIVACY SURVEY 3, 5 (2023), https://perma.cc/EW3Z-Z3SB ("Among this year's respondents, we found that 33% qualified as Privacy Actives, up from 32% in last year's survey, and 29% three years ago. . . . Interestingly, survey results indicate that younger consumers are the most willing to take action when it is necessary to protect their privacy. Forty-two percent of consumers aged 18–34 are Privacy Actives and that percentage steadily decreases with age.").

17 We note, however, that privacy preferences vary across countries. *See* Pinar Akman, *A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets*, 16 VA. L. & BUS. REV. 217, 290 (2022); Jeffrey T. Prince & Scott Wallsten, *How Much Is Privacy Worth Around the World and Across Platforms?*, 31 J. ECON. & MGMT. STRAT. 841, 841 (2022). Indeed, the so-called "privacy paradox" describes how, despite their stated privacy concerns, consumers are readily incentivized to trade their personal data for online services. *See* Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 2 (Nat'l Bureau of Econ. Rsch., Working Paper No. 23488, 2017), https://perma.cc/238F-CT8N.

18 Leah Samuel & Fiona Scott Morton, *What Economists Mean When They Say "Consumer Welfare Standard"*, PROMARKET (Feb. 16, 2022), https://perma.cc/34LG-AEEA ("To academic economists, consumer welfare is the area under the demand curve and above the price paid. This basic concept was popularized by Alfred Marshall in his seminal book *Principles of Economics*, published in 1890. Anything that factors into demand creates consumer welfare: those factors can include price, quality, innovation, privacy, etc."). For a nuanced view of the use of consumer welfare in antitrust, see Barak Y. Orbach, *The Antitrust Consumer Welfare Paradox*, 7 J. COMPETITION L. & ECON. 133, 133 (2010).

19 *See, e.g.*, Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, 40 MKTG. SCI. 661, 680 (2021). According to the authors, the launch and deployment of GDPR provisions were associated with "negative and pronounced effects" on new, data-related venture deals. *Id.*; *see also* Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, *in* 12 INNOVATION POLICY AND THE ECONOMY 65, 65, 86 (Josh Lerner & Scott Stern eds., 2012). The authors discussed how privacy regulations, for example, adversely impacted the deployment of emerging technologies in health. *Id.*

privacy but can have ambiguous total effects on consumer welfare (even considering privacy preferences) when all market adjustments are considered.[20] In studying the impact of the GDPR—which imposed user-consent requirements for data sharing—on webpage views and revenues, the authors estimated a non-consent rate between 4.0% and 12.8%, indicating "that a nonnegligible portion of consumers are benefitting from the ability to opt out of data collection."[21] However, the researchers also found that the GDPR led to a reduction in the number of website page views, likely indicating negative effects on consumer and producer welfare through a contraction in quantity (their analysis is further discussed in the following section).[22]

While the welfare impacts on consumers are nuanced, the effects on firms are more evident: they must comply with the new regulations and otherwise conduct business in a climate of regulatory and enforcement uncertainty. Small businesses are often disproportionately impacted as they navigate the thicket of compliance requirements with fewer resources and less experience.[23] Furthermore, privacy regulations can adversely affect entry by potential rival firms that face prohibitive compliance costs.[24] The potential exit by small firms and decreased entry of new firms can exacerbate market concentration issues, further impacting competitive dynamics.

Moreover, privacy regulations may not always present "tradeoffs" between competition and privacy because it is entirely possible—for example, by increasing market concentration—that privacy-law compliance may lead to less competition and, paradoxically, less desirable privacy outcomes. For instance, Ram Gopal et al. created a crawler that visited the 100,000 highest-traffic websites (according to Alexa.com) and gathered data on third-party usage.[25] Analyzing this data, they found that the CCPA led to an increase in the number of third parties used by the

---

[20] Samuel G. Goldberg, Garrett A. Johnson & Scott K. Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR*, 16 AM. ECON. J.: ECON. POL'Y 325, 325 (2024).

[21] *Id.* at 327.

[22] *Id.* at 350–54.

[23] *Small Business Perspectives on a Federal Data Privacy Framework: Hearing Before the Subcomm. on Mfg., Trade, and Consumer Prot. of the S. Comm. on Com., Sci. & Transp.*, 116th Cong. (2019) [hereinafter *Small Business Perspectives*] (statement of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation) ("[A]s state and federal policymakers look to bolster privacy protections for consumers, there is a very real risk that the end result will be a complex regulatory landscape that startups on bootstrap budgets can't afford to comply with, especially compared to large companies with massive budgets and legal teams.").

[24] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 47 (2015) ("[T]hough privacy regulation imposes costs on all firms, it is small firms and new firms that are most adversely affected.").

[25] Ram D. Gopal, Hooman Hidaji, Sule Nur Kutlu, Raymond A. Patterson & Niam Yaraghi, *Law, Economics, and Privacy: Implications of Government Policies on Website and Third-Party Information Sharing*, 34 INFO. SYS. RSCH. 1375, 1388–89 (2023).

websites.[26] Here, the evidence suggests that the privacy regulation (CCPA) distorted market outcomes in a manner that incentivized greater third-party activity and data sharing, not less.[27] Their analysis points to the importance of accounting for incentive effects that may counter policymakers' objectives.[28]

A subsequent study by Yifei Wang further examined the potential counterproductive impacts of privacy laws that impede competition.[29] Studying the impact of a 2017 Chinese regulation that restricted access to blocked apps which led to a reduction in competition among unblocked apps, Wang identified that the decrease in competition led to an average of 1.46 more privacy permissions and specifically 0.31 more privacy-sensitive permissions among the unblocked apps.[30] Wang's findings indicate that a decrease in competition in the mobile application market can lead to a substantial increase in privacy-intrusive behavior by apps.

Recently, reflecting on the growing evidence, the Organization for Economic Cooperation and Development ("OECD") acknowledged how market concentration can lead to an "infringement of users' data privacy" by large firms engaged in online commerce; for example,

> a firm with strong market power over its end users, whose business model relies on collecting and processing users' data, may have the incentive to reduce the level of data privacy offered to users, and increase data collection to a level that is excessive or unfair, taking advantage of its position to the detriment of consumers.[31]

As discussed above, privacy regulations may ultimately result in decreased consumer privacy through indirect market impacts. However, it is possible that such regulations, on the whole, increase consumer privacy, even if the net welfare effect is negative. Regardless, even if a privacy regulation is, at worst, "privacy neutral" because it does not enhance or worsen user-data protections, such neutrality still comes at the expense of market distortions. Thus, privacy laws, which may not directly embody antitrust objectives, inevitably affect competition and raise antitrust concerns. This interface prompts the following questions: How do privacy regulations impact firms' ability to compete? How do they affect market outcomes and market structure? Do privacy regulations conflict with antitrust laws? The evidence is still filtering in, but the picture it paints so far is that privacy laws can have both welfare-reducing and welfare-increasing competitive effects depending on the situation. Policy analysis, therefore, must account for the antitrust-related welfare

---

26 *Id.* at 1388.

27 *Id.* at 1395.

28 *Id.* at 1396.

29 Yifei Wang, *Competition and Privacy* 1 (Mass. Inst. of Tech. Sloan Sch. of Mgmt., Working Paper No. 4766344, 2023), https://perma.cc/QD53-968W.

30 *Id.* at 3–4.

31 Org. for Econ. Coop. and Dev. [OECD], *The Intersection Between Competition and Data Privacy*, at 13–14, OECD Doc. DAF/COMP(2024)4 (June 13, 2024).

effects of privacy laws in addition to their non-antitrust welfare effects. In the following sections, we review the empirical evidence on these issues.

II. Privacy Regulations and Market Concentration

Privacy and digital regulators and antitrust enforcers must track marketplace developments to assess if privacy regulations potentially lead to greater market concentration. Such regulations may contribute to increased concentration through various channels, such as influencing demand such that users gravitate toward larger providers, increasing entry costs, and imposing compliance burdens that disproportionately impact smaller firms.[32]

The empirical literature provides evidence that such adverse consequences for market concentration may indeed result. This is particularly salient regarding the impact of the GDPR; studies consistently indicate that the GDPR has increased concentration and thereby hurt competition.[33] For example, Julia Schmitt et al. examined web traffic data to study the effect of GDPR enforcement on website usage.[34] The authors analyzed data from SimilarWeb on the top 1,000 Alexa-ranked websites of 13 countries (6,286 websites total) from mid-2017 to the end of 2019.[35] They discovered that less popular websites experienced a decrease in total website visits of 10% to 21%, while more popular websites experienced a relatively limited average decrease of 9%, indicating that GDPR enforcement likely increased market concentration in favor of more popular websites.[36]

Relatedly, Goldberg et al. analyzed the effect of GDPR on website revenue using proprietary Adobe Analytics data.[37] The authors' data spanned two 32-week periods in 2017 and 2018 and covered 1,084 analytics dashboards corresponding to websites serving EU citizens, with a particular focus on e-commerce sites.[38] On average, they estimated a weekly reduction in e-commerce website revenue of 13.3% ($9,227) for the median dashboard.[39] Importantly, they estimated that the decrease in recorded revenue for smaller e-commerce sites was 16.7%, whereas the

---

32 *See Small Business Perspectives*, *supra* note 23.

33 *See* John M. Yun, *A Report Card on the Impact of Europe's Privacy Regulation (GDPR) on Digital Markets*, 31 GEO. MASON L. REV. F. 104, 124 (2024).

34 Julia Schmitt, Klaus M. Miller & Bernd Skiera, *The Impact of Privacy Laws on Online User Behavior* 1 (HEC Paris Bus. Sch., Working Paper No. MKG-2021-1437, 2021), https://perma.cc/86RL-AMLC.

35 *Id.* at 1, 13–14.

36 *Id.* at 41.

37 Goldberg et al., *supra* note 20, at 325.

38 *Id.* at 334.

39 *Id.* at 327.

decline for larger sites was roughly half that number, at 7.9%.[40] The authors also found that smaller firm size corresponded to lower consent rates, which explains the exacerbated revenue drop for smaller firms.[41]

Concerning a distinct, though proximate, web-technology issue, Garrett Johnson et al. demonstrated that the GDPR increased concentration in the web technology market by driving websites to reduce their usage of vendors and gravitate towards "top vendors" (e.g., Facebook- and Google-owned vendors).[42] Analyzing data on over 27,000 high-traffic websites globally and their ties with vendors, the authors found that the GDPR led to a 15% reduction in web technology vendors used by websites and, relatedly, a short-run increase in market concentration of 17%.[43] The authors determined that market concentration was particularly significant among vendors engaged in personal information processing, indicating that personal data collection was more heavily concentrated toward top vendors following the GDPR.[44] Thus, regulations introduced to stymie large-scale flows of personal data to major platforms can instead exacerbate these flows through adverse effects on market concentration.

Adding to these findings, Christian Peukert et al. further studied the short-run impact of the GDPR on the web technology market, using data on more than 110,000 websites.[45] The authors found a "sustained decrease in third-party cookies after the GDPR," indicating a shrunken market for web technology services.[46] The authors described how the dominant vendor—in this case, Google—gained market share in advertising and analytics as other rivals suffered more significant losses, thus exacerbating concentration in the contracted market.[47]

The adverse effects of privacy regulations on market concentration can also result from disproportionate impacts on production costs for smaller firms.[48] For example, Mert Demirer et al. studied the impact of the GDPR on EU firms' cloud data storage (which serves as a production input).[49] Their analysis utilized monthly data from 2016 to 2021 on customers' service usage and expenditures from a major cloud technology

---

40 *Id.* at 328.

41 *Id.* at 355.

42 Garrett A. Johnson, Scott K. Shriver & Samuel G. Goldberg, *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR*, 69 MGMT. SCI. 5695, 5695 (2023).

43 *Id.* at 5715.

44 *Id.*

45 Christian Peukert, Stefan Bechtold, Michail Batikas & Tobias Kretschmer, *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, 41 MKTG. SCI. 746, 746 (2022).

46 *Id.* at 747.

47 *Id.* at 761.

48 Mert Demirer, Diego J. Jiménez Hernández, Dean Li & Sida Peng, *Data, Privacy Laws and Firm Production: Evidence from the GDPR* 43–44 (Nat'l Bureau of Econ. Rsch., Working Paper No. 32146, 2024), https://perma.cc/67P7-29UB.

49 *Id.* at 1.

provider and a panel dataset on cloud adoption covering 3.1 million companies provided by Aberdeen (a market research company).[50] Demirer et al. estimated that the GDPR led to a 20% increase in data storage costs, on average, with the smallest firms facing the highest cost increase (25%) while the largest firms experienced the lowest increase (13%). They concluded that the disparity in cost burden was likely due to the relatively lower resources available to smaller firms for GDPR compliance.[51]

The disproportionate adverse effects of privacy laws on weakly positioned firms—which can exacerbate market concentration—may also be observed through other measures of firm profitability.[52] Mehmet Canayaz et al. analyzed the impact of CCPA adoption on the return on assets ("ROA") of firms that conducted their operations using voice-AI products on devices such as Amazon's Alexa.[53] Analyzing data of over 15,600 conversational voice-AI firms covering a five-year period from January 2017 to February 2022,[54] the authors estimated that, on average, firms with voice-AI products experienced a 1.59% decline in ROA following the CCPA; however, the results varied significantly based on the size of the firms' customer bases.[55] Firms with smaller customer bases saw a substantial decrease in ROA of up to 2.87%, while conversely, firms with larger customer bases experienced a higher ROA after the introduction of the CCPA, providing evidence that "data regulations can entrench incumbents with in-house data."[56] Moreover, the authors found that in addition to firms with small customer bases, nascent and small firms also faced outsized distortionary effects on ROA due to the CCPA.[57]

In addition to disproportionately harming small firms to the benefit of larger firms, privacy regulations can also exacerbate concentration through adverse effects on entry. In the aforementioned study by Jian Jia et al., the authors analyzed technology-venture data from Crunchbase and VentureXpert between 2014 and 2019 to study the effect of the GDPR on new technology firms.[58] The authors determined that for ventures corresponding to more data-reliant products, the monthly number of EU deals (relative to deals in the United States) reduced by 30.7% following

---

50 *Id.* at 11–12.

51 *Id.* at 3–4, 37–38.

52 *See* Mehmet Canayaz, Ilja Kantorovitch & Roxana Mihet, *Consumer Privacy and Value of Consumer Data* 15 (Swiss Fin. Inst., Working Paper No. 22-68, 2022), https://perma.cc/RSE6-KPMB.

53 *Id.* at 1, 21.

54 *Id.* at 3.

55 Canayaz et al., *supra* note 52, at 25–31.

56 *Id.* at 26, 27.

57 *Id.* at 29.

58 *See* Jia et al., *supra* note 19, at 664.

the GDPR rollout.[59] Their findings indicate a negative short-term effect of the GDPR on entry by new data-driven firms.[60]

While the empirical literature generally points to the negative impacts of privacy laws on entry by new firms, a recent study by Xi Wu and Min-Seok Pang indicates that privacy regulations may have differential effects as a function of revenue models and market dynamics.[61] Wu and Pang studied the impact of the GDPR on competition in the iOS mobile app market, utilizing data on the daily top charts (free and paid) of 21 app categories within the EU and United States from January 2015 to December 2019.[62] They observed a decrease in rank volatility and a 27.9% reduction in the number of new apps in the top charts for paid apps in the EU compared to the United States following the enactment of the GDPR, indicating a decrease in competitive intensity within the market.[63] However, Wu and Pang discovered that, after the GDPR, rank volatility increased in the top charts for free apps, and the number of new free apps rose by 14.0% in the EU compared to the United States.[64] Their results imply that the GDPR had an anti-competitive effect in the paid app market but a pro-competitive effect in the free app market.[65] Observing that free-app incumbents depend more heavily on user data monetization, the authors concluded that GDPR's restrictions on data acquisition and usage reduced incumbents' ability to leverage larger, unique datasets, allowing opportunities for new apps.[66] Their conclusion that apps' revenue models significantly determined how the GDPR affected competition suggests that the effects of privacy laws on market concentration may vary depending on specific market characteristics such as business models.[67]

The above study supports the proposition that privacy regulations can potentially have more nuanced effects on market concentration. However, the foregoing review of empirical evidence suggests that privacy regulations tend to exacerbate market concentration, particularly by disproportionately burdening smaller firms and hindering market entry. Ultimately, these dynamics serve to limit market competition, highlighting the tension at the antitrust and privacy interface and

---

59 *Id.* at 672–73.

60 *Id.* at 680.

61 Xi Wu & Min-Seok Pang, How Data Privacy Regulations Affect Competition: Empirical Evidence from Mobile Application Market 25 (Oct. 24, 2021) (unpublished manuscript) (on file with Temple University Fox School of Business), https://perma.cc/5XWW-LMC4.

62 *Id.* at 19.

63 *Id.* at 24.

64 *Id.*

65 *Id.* at 24–25, 37–38.

66 *Id.* at 38–39.

67 Wu & Pang, *supra* note 61, at 39–40.

emphasizing the need for regulator awareness informed by empirical studies on the effects of privacy laws regarding market concentration.

III. Privacy Regulations, Data Tracking, and Digital Advertising

Advertising enables firms to reinforce brand differentiation and alter product demand, increasing their profits and bolstering their competitive standing. Increasingly prevalent and effective, online targeted advertising utilizes "data about individuals to select and display ads or other forms of commercial content."[68] A 2021 study commissioned by the European Parliament found that "[p]otentially as a result of its effectiveness, search engine advertising is the second largest online advertising segment worldwide in terms of revenue with a share of 43.3% in 2019."[69]

A. *Impact of Privacy Laws on Advertising Effectiveness and Profitability*

The effectiveness of personalized, targeted advertising relies substantially on the ability to track data—for example, using cookies, typically across multiple websites.[70] Data tracking provides advertisers with more robust and accurate information regarding valuable consumer characteristics and online activity, allowing advertisers to "target advertising messages to specific consumers at the most beneficial time."[71]

Arslan Aziz and Rahul Telang attempted to measure the "incremental economic value of information that is tracked by cookies," thereby determining the value of data tracking in ad targeting.[72] To do so, they analyzed 1.3 million bid requests received by a digital advertising firm that tracked information on user purchases and interactions via cookies.[73] The authors estimated several logistic model specifications to predict purchases, encompassing increasingly more observed cookie variables (e.g., browser type, number of impressions served over the last day, and

---

[68] EU Directorate-Gen. for Internal Pol'ys, Dep't for Citizens' Rts. & Const. Affs., *Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent*, at 1–2, PE 696.967 (2021). The authors note that "[a] complex online advertising ecosystem has emerged that besides marketers and targeted individuals involves further actors: publishers and different advertising intermediaries, such as advertising networks, advertising exchanges, supply-side and demand-side platforms, and data management companies (platforms, brokers, data analytics, and market research companies)." *Id.* at 2.

[69] EU Directorate-Gen. for Internal Pol'ys, Dep't for Econ., Sci. & Quality of Life Pol'ys, *Online Advertising: The Impact of Targeted Advertising on Advertisers, Market Access and Consumer Choice*, at 16, PE 662.913 (2021).

[70] *See* Acquisti, *supra* note 11, at 12.

[71] *See id.*

[72] Arslan Aziz & Rahul Telang, *What Is a Digital Cookie Worth?* 1, 32 (Carnegie Mellon Univ., Working Paper, 2016), https://perma.cc/N5FX-B8UR.

[73] *Id.* at 13.

date of last purchase from the advertiser).[74] Aziz and Telang determined that the model's accuracy in predicting purchases, and thereby advertisers' ability to target, increased as more variables were utilized for prediction. The authors also discovered that using more intrusive models for targeting advertising could further "substantially increase ad effectiveness."[75] For example, including more "intrusive" information that captured interactions between end users and advertisers' products (including purchase histories) increased predicted incremental sales by approximately 85%.[76] Therefore, the authors concluded that advertisers' access to more intrusive consumer information could be crucial in improving both ad targeting and targeted ad effectiveness.[77]

The importance of consumer information as an input for targeted advertising is further reflected in private firms' valuation of user data. For example, Michael Kummer and Patrick Schulte empirically analyzed app privacy permissions and concluded that cheaper apps required more privacy-sensitive permissions.[78] The authors analyzed monthly data on 300,000 apps obtained from the Google Play Store in 2012 and 2014 and quantified price reductions associated with privacy sensitivity.[79] Their results suggested that "developers are willing to reduce the app price by about 12% if the app has a privacy-sensitive permission."[80] The authors concluded that their findings demonstrate the importance of user data as an input that "enhances the effectiveness of targeted advertisement" by illustrating the substantial monetary value that app developers place on consumer data.[81]

Foreseeably, therefore, many additional empirical studies point to the reduced effectiveness of online advertising when privacy regulations hinder data tracking and the collection of personal information.[82] A 2011 study by Avi Goldfarb and Catherine Tucker examined the impact of the "ePrivacy Directive," Directive 2002/58/EC of the European Parliament, on advertising effectiveness.[83] This Directive established "rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications" and prohibited

---

74 *Id.* at 16–17.

75 *Id.* at 29.

76 *Id.*

77 *Id.* at 31.

78 Michael Kummer & Patrick Schulte, *When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications*, 65 MGMT. SCI. 3470, 3470 (2019).

79 *Id.* at 3474.

80 *Id.* at 3487.

81 *See id.* at 3472.

82 *See* Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57, 57 (2011); Catherine E. Tucker, *The Economics of Advertising and Privacy*, 30 INT'L J. INDUS. ORG. 326, 327 (2012).

83 Goldfarb & Tucker, *supra* note 82, at 58.

"unsolicited communications where the user has not given their consent."[84] In particular, the Directive discussed a "data subject's consent" requirement that could "be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."[85]

To examine the impact of the ePrivacy Directive on online advertising, Goldfarb and Tucker compiled a global dataset corresponding to 9,596 studies of online ad campaigns, covering 2001 to 2008;[86] these studies assessed the effectiveness of the campaigns through surveys in which respondents reported their intent to purchase.[87] Based on the results of the studies, the authors estimated that the ePrivacy Directive was followed by a substantial average decrease in advertising effectiveness of 65%.[88]

Thus, there is considerable evidence that privacy regulations—particularly through limiting data collection and utilization—can harm firms engaged in e-commerce by vitiating ad effectiveness and undermining the viability of an ad-driven revenue model. However, we note that there may be instances where the effects are not unidirectional, as indicated by Guy Aridor et al.'s, "The Effect of Privacy Regulation, " 2023, examination of the impact of user-consent requirements under the GDPR on advertisers.[89] In their examination, the authors utilized data on search queries and purchases made by consumers in 2018 across online travel agencies.[90] The authors found a 12.5% reduction in total cookies, indicating that consumers employed the capability offered by the GDPR not to opt in; however, despite the reduction in cookies, the trackability of remaining consumers increased by 8.0%.[91] Driven by the increased trackability of those who opt in, the authors' empirical analysis indicates that "[o]verall, . . . [the] GDPR has not negatively impacted the ability to predict consumer behavior . . . ."[92] Nevertheless, their analysis does show that "smaller advertisers . . . are able to collect less data and conduct less business due to consumer opt-out."[93]

---

84 *Data Protection in the Electronic Communications Sector*, EUR. UNION, https://perma.cc/9F6Q-FCKX (May 25, 2020).

85 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, 38.

86 Goldfarb & Tucker, *supra* note 82, at 61.

87 *Id.* at 62.

88 *Id.* at 64.

89 Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR*, 54 RAND J. ECON. 695, 695 (2023).

90 *Id.* at 705.

91 *Id.* at 697.

92 *Id.* at 718.

93 *Id.* at 719.

In summary, privacy regulations can negatively impact ad effectiveness and profitability, leading to an entrenchment of larger digital advertisers and a rise in prices. Therefore, regulations designed to address valid consumer privacy concerns regarding online targeted advertising may impart unintended harm to consumers, suggesting that the net welfare effect is not necessarily positive.

B. *Lessons from Private Contracting and Competition*

Regulators can also seek guidance from instances where firms have privately designed and deployed data protections. Consider Google's Privacy Sandbox, launched in 2019 to "fundamentally enhance" internet privacy, as an illustrative case study.[94] Notably, the initiative featured a "plan to phase out support for third-party cookies in Chrome."[95] In its 2020 report on competition in digital markets, the U.S. House of Representatives Antitrust Subcommittee pointed to market participants' concerns that while other advertisers relied on third-party cookies and thus would face significant data collection challenges from the Privacy Sandbox, Google could continue to leverage data it gathered through its digital ecosystem.[96] Miguel Alcobendas et al. described this effect as facilitating an "information monopoly."[97] To study the impact of Google's proposed ban on third-party cookies on the online advertising supply chain, the authors analyzed Yahoo ad auction data comprising over 5.5 million bids from about 737,000 auctions.[98] In particular, using a simulation study, they determined that advertisers using Demand-Side Platforms ("DSPs") experienced an overall 40.0% decrease in surplus; however, the distributional effect was found to be highly unequal among large, informationally advantaged bidders and smaller (informationally

---

[94] Justin Schuh, *Building a More Private Web*, GOOGLE: THE KEYWORD (Aug. 22, 2019), https://perma.cc/BCA9-GY75.

[95] Justin Schuh, *Building a More Private Web: A Path Towards Making Third Party Cookies Obsolete*, CHROMIUM BLOG (Jan. 14, 2020), https://perma.cc/RAP6-FWA4; *see Privacy Sandbox for the Web*, PRIVACY SANDBOX, https://perma.cc/3UGX-54WC (last updated Aug. 2024) (stating in the "Third-Party Cookie Phase Out" pop-up that "[w]e envision proceeding with third-party cookie deprecation starting early 2025, subject to resolving any remaining concerns with the CMA.").

[96] MAJORITY STAFF OF SUBCOMM. ON ANTITRUST, COM. & ADMIN. L., H. COMM. ON JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 230 (Comm. Print 2020) ("Several observers have noted that this change would have the likely effect of reinforcing Google's power and harming rivals, shifting more advertisers toward Google. In particular, market participants are concerned that while Google phases out third-party cookies needed by other digital advertising companies, Google can still rely on data collected throughout its ecosystem.") (footnote omitted).

[97] Miguel Alcobendas, Shunto J. Kobayashi, Ke Shi & Matthew Shum, The Impact of Privacy Protection on Online Advertising Markets 2 (Oct. 6, 2023) (unpublished manuscript) (on file with authors), https://perma.cc/4F54-ZPRA.

[98] *Id.* at 10–11.

disadvantaged) bidders.[99] The authors quantified the extent to which the ban on third-party cookies in ad auctions benefited large, informationally advantaged participants by analyzing the bidding decisions of DSPs.[100] To do so, they performed a second simulation exercise that considered the effect of an asymmetric ban in which a large, general-purpose ("Big Tech") DSP (e.g., Google's DSP) retained access to Chrome user information following the ban.[101] In this case, the authors found that the Big Tech DSP's winning frequency increased from 8.3% in the benchmark (no-ban) scenario to 15.4% in the case of an asymmetric ban; furthermore, their total surplus increased by more than 54.0%.[102] In contrast, all other bidders' winning frequencies and total surpluses decreased due to the ban.[103] Thus, the authors concluded that the "plan to eliminate third-party cookies raises legitimate antitrust concerns regarding competition and monopoly power in online advertising markets."[104]

Offering a second illustrative case study, Apple's AppTrackingTransparency ("ATT")[105] "mandates iOS apps to ask users' permission to track their activity across other apps and websites."[106] Similar to a regulation that requires online businesses to allow consumers to opt out of being tracked, Apple implemented a mechanism enabling iOS users to opt out of tracking using third-party mobile applications, which it began enforcing in 2021.[107]

Foretelling the impacts of ATT, a study of Apple's earlier Intelligent Tracking Prevention ("ITP"), which preceded ATT and changed default settings without informing users, revealed adverse outcomes for competitors. Using data from a large web publisher, Ramnath K. Chellappa et al. studied approximately 21 million ad impressions that

---

99 *Id.* at 30. A Demand Side Platform ("DSP") provides a software system that automates purchases of ad impressions. *See* Shivani Salhotra, *Demand Side Platform (DSP): A Simple Explanation*, REVX (Apr. 28, 2020), https://perma.cc/9Y8V-TZYC.

100 Alcobendas et al., *supra* note 97, at 3.

101 *Id.* at 3–4, 29. For a real-world example of a Big Tech DSP retaining access to user information, see *Display & Video 360*, GOOGLE: MKTG. PLATFORM, https://perma.cc/L3N5-B7JS.

102 Alcobendas et al., *supra* note 97, at 30–32.

103 *Id.* at 32.

104 *Id.* at 35–36.

105 *See User Privacy and Data Use*, APPLE DEV., https://perma.cc/W4NU-WL8M ("In iOS 14.5, iPadOS 14.5, and tvOS 14.5 or later, you need to receive the user's permission through the AppTrackingTransparency (ATT) framework in order to track them or access their device's advertising identifier. Tracking refers to the act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers.").

106 *See* Jacob Loveless, *How Does Apple's App Tracking Transparency Framework Affect Advertisers?*, FORBES (Aug. 22, 2022, 10:15 AM), https://perma.cc/Y3YD-9M6B.

107 *Upcoming AppTrackingTransparency Requirements*, APPLE DEV. (Apr. 20, 2021), https://perma.cc/667D-9QBB.

appeared on iOS devices within twelve weeks before and after the introduction of ITP.[108] The authors estimated that the ITP policy led to a notable decrease in ad effectiveness, as evidenced by an 18.8% reduction in click-through odds across all advertisers, with small and mid-sized businesses experiencing a more pronounced effect (30.0%).[109] Thus, the authors found that the ITP policy reduced the benefits of digital advertising, with disproportionately adverse effects on smaller advertisers.[110]

Following the ITP, the introduction of the ATT framework also led to adjustments in firms' strategies; for example, the empirical evidence suggests that app developers considered alternative routes to monetization. A study by Reinhold Kesler examined a potential alteration in app developer conduct regarding in-app payments and above-zero purchase prices as alternative revenue sources following the introduction of ATT.[111] The author examined web-scraped data from February 2021 to December 2021 of approximately 580,000 iOS apps and 900,000 Android apps;[112] for each app, Kesler collected comparable information on the primary measures of monetization, reliance on Apple, and dependence on data tracking.[113]

Performing a before-after and difference-in-difference analysis of iOS apps against Android apps, Kesler demonstrated that ATT increased the prevalence of paid apps and reinforced the industry trend toward increased in-app payments.[114] The impact was particularly pronounced among apps relying on Apple, employing user tracking, or targeted explicitly by ATT.[115] Kesler concluded that this could "bring about a compositional change and along with analyses showing increased exit of apps without payments and increased (new) entry of apps with payments around and following ATT, it sheds light onto the possible long-run impact."[116]

Cristobal Cheyre et al. offered additional, more complex evidence of the effect of ATT on app developers.[117] They analyzed data on roughly

---

108 Ramnath K. Chellappa, Jonathan Gomez Martinez & Gordon Burtch, In the Name of Privacy - The Impact of Apple's Intelligent Tracking Prevention (ITP) on the Advertising Ecosystem: *Cui Bono*? 7 (Mar. 30, 2024) (unpublished manuscript) (on file with authors).

109 *Id.* at 9.

110 *See id.*

111 Reinhold Kesler, The Impact of Apples App Tracking Transparency on App Monetization 2 (Aug. 8, 2023) (unpublished manuscript) (on file with authors), https://perma.cc/DP2C-9BYL.

112 *Id.* at 9–10.

113 *Id.* at 10–12.

114 *Id.* at 16–17.

115 *See id.* at 19–21.

116 *Id.* at 24.

117 *See* Cristobal Cheyre, Benjamin T. Leyden, Sagar Baviskar & Alessandro Acquisti, *The Impact of Apple's App Tracking Transparency Framework on the App Ecosystem* 1 (CESifo, Working Paper No. 10456, 2023), https://perma.cc/Z2B5-CM9M.

seven million zero-price apps available for download from Apple's App Store and Google's Play Store.[118] Using a difference-in-difference analysis, they found that the introduction of ATT was initially associated with a relative decrease in the number of available Apple apps;[119] however, the availability of active apps subsequently rebounded within a few months.[120] Their findings suggest that ATT did not have a long-run negative effect on the availability of mobile applications. Nevertheless, the authors identified fundamental changes in firm conduct; analyzing the use of Software Development Kits ("SDKs") by apps, the authors found a decrease in the use of Ad Mediation and Monetization SDKs and an increase in the utilization of Payments and Authentication SDKs.[121] Furthermore, while discrediting the potentially negative impact of ATT on app availability, the authors confirmed several other adverse industry impacts. For example, the number of developers' app updates decreased, possibly pointing to a decrease in investment.[122] Additionally, the authors reported a decline in the number and score of ratings received by existing apps, implying a lower user valuation of these apps.[123] Therefore, as the authors concluded, the absence of ATT effects on the long-term availability of apps contradicted industry concerns; however, the policy likely altered firm conduct and possibly decreased developer investment in and user valuation of the apps.

Shedding further light on the effects of ATT on firm conduct and competition, Guy Aridor et al., "Evaluating the Impact of Privacy Regulation," 2024, studied the impact of ATT on Meta ads.[124] The authors utilized multiple data sources, including information on global firm-level traffic and revenues and data on ad spending and performance across Meta, Google, and TikTok.[125] Performing a difference-in-difference analysis, they found that ATT significantly diminished the effectiveness of advertising targeted using third-party data, observing a 37.1% reduction in click-through rates for advertising campaigns employing third-party data relative to campaigns optimized based on first-party data.[126] Similarly, Grazia Cecere and Sarah Lemaire conducted an experiment in which they utilized the Facebook marketing API to compare changes in both iOS and

---

118 *Id.* at 7–8.

119 *Id.* at 10.

120 *Id.*

121 *Id.* at 15.

122 *Id.* at 3.

123 Cheyre et al., *supra* note 117, at 3.

124 Guy Aridor, Yeon-Koo Che, Brett Hollenbeck, Maximilian Kaiser & Daniel McCarthy, Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency 3 (June 13, 2024) (unpublished manuscript) (on file with authors), https://perma.cc/H9CV-4L2E.

125 *Id.* at 9.

126 *Id.* at 16–17.

Android to analyze targeting efficiency and pricing for digital advertising.[127] After the introduction of ATT, they found that targeted advertising decreased in effectiveness; specifically, they determined that ATT led to 7.5% fewer actions per impression for iOS users, while for Android users, the number of actions per impression decreased by 10.0%.[128]

As a final warning, ATT also serves as a case study illustrating how platform owners can potentially leverage their market power to mimic third-party complementors and launch similar products, thereby entrenching their dominant position.[129] To examine this potential effect pertaining to ATT, Tommy Fang analyzed a sample of over 15,600 mobile applications and 12 ad networks between January and July 2021.[130] The author discovered that third-party complementors decreased new value-creation activities due to the introduction of ATT.[131] As a result, the overall platform value capture for such apps decreased,[132] while the platform value captured by Apple's apps and ad networks increased.[133]

Paralleling the evidence, certain regulators voiced concerns regarding the potential anti-competitive implications of user-data protections provided by ATT. For example, France's *Autorité de la Concurrence* raised concerns that, through ATT, Apple would "abuse its dominant position by implementing discriminatory, non-objective and non-transparent conditions for the use of user data for advertising purposes."[134] In the United Kingdom, the Competition and Markets Authority noted that "Apple's App Tracking Transparency policy gives Apple device users greater control over their personal data, enhancing privacy and choice. However, the way it has been implemented . . . may distort user choice, potentially tilting the playing field in Apple's [favor] in respect of app discovery and advertising services."[135] And Germany's *Bundeskartellamt* "initiated a proceeding against the technology company Apple to review

---

127 *See* Grazia Cecere & Sarah Lemaire, Have I Seen You Before? Measuring the Value of Tracking for Digital Advertising 1 (Dec. 10, 2023) (unpublished manuscript) (on file with authors), https://perma.cc/249K-3YN3.

128 *Id.* at 3.

129 *See* D. Daniel Sokol & Feng Zhu, *Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates*, 107 CORNELL L. REV. ONLINE 94, 96 (2022).

130 *See* Tommy Pan Fang, Managing Platform Value Through Business Model Governance 1, 14 (July 9, 2024) (unpublished manuscript) (on file with author).

131 *Id.* at 26–27.

132 *See id.* at 27.

133 *Id.*

134 *See French Antitrust Watchdog Issues Statement of Objection Over Apple App Tracking*, REUTERS (July 25, 2023, 5:41 PM), https://perma.cc/79J6-HSLM.

135 COMPETITION & MKTS. AUTH., MOBILE ECOSYSTEMS: MARKET STUDY FINAL REPORT, 2022, at 181 (UK), https://perma.cc/L7HC-JVHL.

under competition law its tracking rules and the App Tracking Transparency Framework."[136]

Regulator's concerns of ATT regarding self-preferencing and the entrenchment of large players—substantiated by the foregoing review of the empirical evidence—suggest that, in turn, policymakers would do well to learn from the data in assessing whether the public provision of personal data protection may entail a parallel set of antitrust concerns.

IV. Data Portability and Platform Interoperability

In this Section, we examine the competitive impacts of privacy laws that grant consumers enhanced control over their data beyond data-collection consent requirements. In particular, data portability provisions grant consumers the right to access personal data that online businesses may have collected and stored. For example, the CCPA permits consumers to request that businesses disclose the categories and sources of collected personal information, the reasons for collecting and selling personal data, information concerning third parties receiving users' data, and the types of personal information collected.[137]

The GDPR established Data Portability as a global digital privacy rights standard in 2016. Article 20 ("Right to data portability") of the GDPR provides that a

> data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.[138]

Data Portability compliance naturally intersects with competition policy. For example, in 2022, the Italian Competition Authority (Autorità Garante della Concorrenza e del Mercato), alleged that Google had not sufficiently complied with Article 20 of the GDPR by utilizing its dominant market position to limit interoperability with other platforms.[139] According to the Italian Competition Authority, Google's restriction of data sharing could suppress data portability and undermine competition (among other effects), thereby entrenching its market power.[140] The investigation was closed in July 2023 after Google

---

136 Press Release, Bundeskartellamt, Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps (June 14, 2022), https://perma.cc/X3UB-CJR9.

137 *See* CAL. CIV. CODE § 1798.110(a) (West, Westlaw through Ch. 1002 of 2024 Reg. Sess.).

138 GDPR, *supra* note 1, at 45.

139 *See* Press Release, Autorità Garante della Concorrenza e del Mercato, A552 - Italian Competition Authority, Investigation Opened Against Google for Abuse of Dominant Position in Data Portability (July 14, 2022), https://perma.cc/LBG6-6XDR.

140 *Id.*

committed to undertake measures to ensure extensive automation of the data-export procedure.[141]

Besides the provision's inherent "privacy rights" value, data portability ostensibly fosters competition by lowering switching costs since consumers can more easily obtain and transfer their information from one service to another. However, the OECD has cautioned that data portability and interoperability measures pursued with non-competition objectives may not foster competition "unless designed with market dynamics in mind."[142]

Validating this concern, Emmanuel Syrmoudis et al. studied various dimensions (such as file formats, data scope, transfer duration, etc.) along which online services complied with the GDPR's Right to Data Portability ("RtDP").[143] The authors determined that more popular websites were more likely to comply with data portability provisions and require a greater number of authentication factors to verify the requester's identity;[144] moreover, a significant, positive relationship was found between website popularity and scope of data exported to individuals and import possibilities offered to them.[145] These results indicate that "[i]ncumbents . . . seem to know better how to use the RtDP for defending their positions by building enhanced trust with consumers, which in turn can lead to them providing more data."[146] Thus, the authors concluded the presence of a "data portability divide, in which," on one side, "a few large incumbents strategically make use of the advantages that data portability can bring to them," while "[o]n the other side of the divide, a majority of corporations try to comply with a regulation whose economic implications they do not seem to grasp . . . ."[147]

Privacy regulations tailored to the particular market dynamics of a specific sector may offer greater potential for pro-competitive impacts, and the deployment of data portability provisions in the FinTech industry offers a valuable example of this sectoral approach. Open banking comprises "a set of initiatives by governments and industry to implement data portability and improve users' access to financial information and

---

141 *See* Press Release, Autorità Garante della Concorrenza e del Mercato, A552 - Italian Competition Authority: Following the Authority's Intervention, Google's Data Portability Becomes Easier (July 31, 2023), https://perma.cc/5ZV3-R7PG.

142 Org. for Econ. Coop. & Dev. [OECD], *OECD Competition Committee Discussion Paper: Data Portability, Interoperability and Digital Platform Competition*, at 49 (2021), https://perma.cc/XQ74-T393.

143 Emmanuel Syrmoudis, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags & Johann Kranz, *Data Portability Between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, PROC. PRIV. ENHANCING TECHS., July 2021, at 351, 355–57.

144 *Id.* at 361.

145 *Id.* at 361–63.

146 *Id.* at 366.

147 *Id.* at 364 (emphasis omitted).

services, while preserving privacy and security."[148] Thus, customers are given greater control over their financial data, including accessing and managing data and granting permissions or sharing data with authorized third parties for improved and personalized finance offerings.[149] A recent study by Rachel Nam of a sample comprising over 18 million loan applications in Germany between 2018 and 2022 (when open-banking data-sharing regulations were already in place in Germany) also revealed that, in addition to enhanced consumer control over their transaction information, data sharing increased the loan approval probability and decreased interest rates across all credit-score groups.[150] The results regarding approval probability and interest-rate effects generally indicate pro-competitive impacts of data sharing.

Overall, this Section on the competitive impacts of data portability provisions echoes the general theme developed through reviewing the empirical evidence presented in the preceding sections. In general, the effects of these provisions on competition can be mixed, and there is evidence that more entrenched, larger online businesses may leverage compliance to the detriment of smaller players. This may result from decreased compliance (e.g., limited interoperability) among firms but increased compliance with consumers (e.g., expanding data sharing to build trust). However, FinTech's experience with data portability provisions provides regulators with a case study showing that a tailored, sectoral approach may offer better opportunities for a pro-competitive deployment of privacy rules.[151]

---

148 Org. for Econ. Coop. & Dev. [OECD], *Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues*, at 5, OECD Doc. DSTI/CDEP/DGP/2022/11/FINAL (Feb. 22, 2023), https://perma.cc/WRP9-24S3.

149 *Id.*; *see also* Bill Roberts, Head of Open Banking, U.K. Competition & Mkts. Auth., Remarks at Data to Go: An FTC Workshop on Data Portability (Sept. 22, 2020) (transcript on file with authors), https://perma.cc/FR84-XAZ3 ("So by open banking, we're referring to an ecosystem in which consumer[s] or small businesses can, first of all, instruct a bank to share their transaction data securely with a third party, and, [second of all], instruct a third party to move money around in and out of that bank account. So open banking allows consumers to take control of their own bank data.").

150 Rachel J. Nam, *Open Banking and Customer Data Sharing: Implications for FinTech Borrowers* 11, 33 (Leibniz Inst. for Fin. Rsch. SAFE, Working Paper No. 364, 2024), https://perma.cc/SLP9-TP5R.

151 *See, e.g.*, *Data To Go: An FTC Workshop on Data Portability*, FED. TRADE COMM'N, https://perma.cc/UF9A-CGLT. By 2020, the Federal Trade Commission had already asked:

> Does data portability work better in some contexts than others (e.g., banking, health, social media)? Does it work better for particular types of information over others (e.g., information the consumer provides to the business vs. all information the business has about the consumer, information about the consumer alone vs. information that implicates others such as photos of multiple people, comment threads)?

Id.

Conclusion

As regulators increasingly regard consumers' privacy protections as a means to a pro-competitive end, there is a tendency toward a coupling of antitrust and privacy protections. The purpose of this Article is to highlight to regulators that the empirical reality is more complicated.

The objectives of privacy regulations are not under question; however, the effects of these regulations must be scrutinized and analyzed to inform sound regulatory design and reform. In particular, sweeping privacy legislation or even private governance of platforms can significantly alter firms' incentives and costs, which affect contracting, pricing, market structure, entry, exit, etc. The empirical evidence reviewed in this Article further underscores that these effects may be differentiated depending on the time horizon, nature of policy intervention, and industry. In doing so, privacy regulation and governance may entail adverse consequences not just for competition but for privacy as well, with the ultimate result that consumers are left worse off than before.

The picture is not one-sided; regulators would do well to identify opportunities to increase privacy (e.g., personal data protection) such that the net effect on competition is positive. Experience tells us that the deployment of privacy laws has the potential to benefit consumers but also the capacity to disrupt markets and negatively affect competition (and market participants, including these consumers).

Consequently, the design of privacy laws must be guided by a framework that provides for a robust analysis of their competitive effects. This Article has offered regulators an ex-post review of the empirical effects of these laws and both public and private regulations. Only through a better understanding of the costs and benefits of the empirics of the interface of competition and privacy can enforcers and regulators create more effective policy choices.