Privacy Law's Incumbency Problem

Peter Ormerod[*]

Policymakers and scholars concerned with the power of informational platforms are questioning how traditional doctrinal silos like privacy law and antitrust law interact in digital markets. Their interaction has taken on new urgency in recent years as states have enacted a flurry of consent-based privacy laws and as digital markets have become increasingly dominated by the same few firms.

Contemporary debates about the interaction of competition and privacy tend to ask what role, if any, privacy should play in the antitrust analysis. Little has been written about how new privacy laws shape the competitive landscape. This Article argues that consent-based privacy laws confer three distinct powers on entrenched incumbent firms.

The first is the power to comply. Dominant firms realize economies of scale in any regulatory compliance regime, but they are uniquely advantaged by the need to obtain consent to collect and process users' information. The second is the power to restrict. By constraining information flows, privacy laws deprive insurgents of access to data that could prove valuable in challenging incumbents' dominance, and consent mechanisms exacerbate the dynamic by supplying incumbents with a legal justification for refusing to share their data and circumscribing competitors' access to it. The third is the power to circumvent. A private-sector initiative that limits the collection and sharing of advertising-related information shows that stringent consent mechanisms may

 Assistant Professor of Law, Northern Illinois University College of Law. My thanks to Jeffrey Bellin, Bryan Choi, Greg Elinson, Margaret Kwoka, Kirsten Martin, Ben Sobel, Jim Speta, Olivier Sylvain, and Jordan Wallace-Wolf for their comments and feedback on earlier versions. I'm also grateful to the participants in 2024 Privacy Law Scholars Conference, the Sixth Annual Chicagoland Junior Scholars Conference, the Ohio State University Moritz College of Law Information Governance Colloquium, and a faculty workshop at the Northern Illinois University College of Law.

deprive all firms of some data, but incumbents with sufficient scale — and only such firms — can circumvent and overcome these restrictions.

Taken together, the three powers of incumbency suggest that laws like the California Consumer Privacy Act will further entrench dominant informational platforms like Meta's and Google's — and they thereby raise difficult questions for those who seek to curb platform power. Ultimately, privacy law's incumbency problem suggests pessimism about pursuing competition to the exclusion of other policies and about the prevailing approach to privacy law.

TABLE OF CONTENTS

INTRODUCTION

In the past generation, a small number of technology companies have come to dominate a staggering degree of modern life. Just five companies — Amazon, Apple, Google, Meta, and Microsoft — exercise unprecedented control over the devices we use, our interactions with one another, how we acquire information, how we entertain ourselves, what kinds of goods and services we purchase, the tools we use to earn a living, and the ways in which our attention is bought and sold. Microsoft and Apple own the operating system on nine out of every ten computers, and Apple and Google own the operating system on ninety-nine percent of mobile devices.[1] Amazon's share of e-commerce is six times the size of its nearest competitor,[2] and Amazon, Google, and Meta earn six out of every ten dollars spent on digital marketing.[3] Google's search and mapping products each command eighty-plus percent of their respective markets,[4] while Google Chrome and Apple's Safari

[1] *See* Ahmed Sherif, *Global Market Share Held by Operating Systems for Desktop PCs, from January 2013 to February 2024*, STATISTA (Mar. 5, 2024), http://statista.com/statistics/218089/global-market-share-of-windows-7/ [https://perma.cc/7375-TAKN]; Ahmed Sherif, *Market Share of Mobile Operating Systems Worldwide from 2009 to 2024, by Quarter*, STATISTA (May 13, 2024), http://statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ [https://perma.cc/9DSK-EL9W].

[2] *See* Stephanie Chevalier, *Market Share of Leading Retail E-Commerce Companies in the United States in 2023*, STATISTA (May 22, 2024), http://statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/ [https://perma.cc/MEL5-5PXT].

[3] *See Share of Major Ad-Selling Companies in Digital Advertising Revenue in the United States from 2021 to 2026*, STATISTA (June 25, 2024), http://statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/ [https://perma.cc/78CB-7GDE].

[4] *See* Tiago Bianchi, *Market Share of Leading Desktop Search Engines Worldwide from January 2015 to January 2024*, STATISTA (May 22, 2024), http://statista.com/statistics/216573/worldwide-market-share-of-search-engines/ [https://perma.cc/4RKA-4UTM] (search); Laura Ceci, *Most Popular Mapping Apps in the United States as of April 2018, by Reach*, STATISTA (Aug. 25, 2023), http://statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/ [https://perma.cc/QL7B-EJXE] (Google owns Google Maps, Waze, and Google Earth).

together possess a similar share of web browsers.[5] Nearly eighty percent of American teens report that they use YouTube at least once a day.[6]

There are few historical examples of such vast power being concentrated in the hands of small number of executives who are duty-bound to seek the wealth maximization of their shareholders.[7] But that's not the only novel facet of today's technology giants: they also govern the global information ecosystem,[8] and they all generate substantial value from processing personal information on a scale that would have been inconceivable at the time each was founded.[9] The companies

[5] *See* Lionel Sujay Vailshery, *Market Share Held by Leading Internet Browsers in the United States from January 2015 to May 2024*, STATISTA (June 21, 2024), http://statista.com/statistics/545520/market-share-of-internet-browsers-usa/ [https://perma.cc/ZH4N-MV7N].

[6] *See* Emily A. Vogels & Risa Gelles-Watnick, *Teens and Social Media: Key Findings from Pew Research Center Surveys*, PEW RSCH. CTR. (Apr. 24, 2023), http://pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/ [https://perma.cc/8AYC-XS5C].

[7] The closest historical analogs to the big five technology companies enumerated above — in terms of the comparative and absolute populations regularly affected by their decisions — are probably the British East India Company and the Dutch East India Company. *See* Evelyn Douek (@evelyndouek), X (Sept. 30, 2021, 10:43 AM) https://x.com/evelyndouek/status/1443602304079388675 [https://perma.cc/834P-33BE].

[8] The big five tech companies enumerated above all have robust content-moderation regimes that govern how billions of people access information on a day-to-day basis. *See* Rebecca Aydin, *Amazon, Facebook, Twitter, and YouTube Are All Facing Moderation Issues — Here's How America's Tech Giants Are Struggling to Police Their Massive Platforms*, BUS. INSIDER (Aug. 24, 2019, 7:23 AM), https://www.businessinsider.com/amazon-youtube-twitter-facebook-content-moderation-issues-2019-8 [https://perma.cc/D69F-TH7V]; *see also App Review Guidelines*, APPLE, https://developer.apple.com/app-store/review/guidelines/ (last updated Aug. 1, 2024) [https://perma.cc/TFX6-5SKH] (categorizing "[o]vertly sexual or pornographic material" as "objectionable," and thereby prohibiting it).

[9] The big five tech companies enumerated above were founded between 1975 and 2004, and all five companies — as a function of offering software products and services to billions of people — process vast quantities of user data. Council Regulation 2016/679, art. 4(2), 2016 O.J. (L 119) 1 [hereinafter GDPR] (defining "processing"); *see also* Rachyl Jones, *Five Years into the GDPR, Few Say It's Working and Meta is Paying Big*, OBSERVER (May 15, 2023, 5:00 AM), https://observer.com/2023/05/gdpr-europe-meta-fines/ [https://perma.cc/F33T-TW3N] (conveying that all five big tech companies are subject to the GDPR). Only a prescient few foresaw digital technologies' capacity for today's volume of data processing. *See, e.g.*, VINCENT MOSCO, *Introduction: Information in the Pay-*

leverage their advantage and wield that information to profitably predict and modulate our behavior.[10]

As these companies have amassed more wealth and power, policymakers have become increasingly skeptical of the long-held consensus that less regulation of them is preferable.[11] A month after the European Union implemented the General Data Protection Regulation ("GDPR") in 2018, the California legislature responded to a looming ballot initiative by enacting the first domestic omnibus privacy law.[12] Unlike past privacy laws that regulate specific types of information and specific types of actors,[13] the California Consumer Privacy Act ("CCPA") provided consumers with a series of individual privacy rights and entitled them to assert those rights against a wide array of for-profit businesses that collect and process their information.[14] The GDPR and CCPA both hinge on consent: so long as the regulated entities obtain it, they have free rein to process users' information however they please.[15] This approach — pairing user control rights and consent-as-an-inoculation with a generally applicable consumer privacy law — has proved incredibly influential: in the past five years, an additional eighteen states have enacted laws modeled off the CCPA.[16]

State-level privacy laws have been the most prolific regulatory initiative to date, but they aren't the only front in the ongoing contest

per Society, *in* THE POLITICAL ECONOMY OF INFORMATION 3, 5-6 (Vincent Mosco & Janet Wasko, eds., 1988).

[10] *See infra* notes 255–256 and accompanying text.

[11] *See* Roger P. Alford, *The Bipartisan Consensus on Big Tech*, 71 EMORY L.J. 893, 904 (2022).

[12] GDPR, *supra* note 9; *see* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/43G7-YDL5].

[13] *See, e.g.*, WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 669-70 (Saul Levmore et al. eds., 2d ed. 2023) (describing the "hodgepodge" of US data protection laws).

[14] *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (2018); *see also* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734 (2021).

[15] *See infra* notes 53–55 and accompanying text.

[16] *See* Andrew Folks, *US State Privacy Legislation Tracker*, IAPP, http://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Jul. 22, 2024) [https://perma.cc/6SDS-868M].

between policymakers and large technology companies.[17] As digital markets have become increasingly concentrated, scholars and policymakers have sought to target firms' dominance by reclaiming antitrust law from the neoclassical Chicago School.[18] This Neo-Brandeis movement rejects the Chicago School's narrow focus on prices and consumer welfare, opening the competition-law aperture to considerations like labor-market effects and competition over non-price quality parameters.[19] In recent years, policymakers have increasingly made Neo-Brandeis arguments in merger decisions and anti-monopoly enforcement actions.[20]

Privacy law and antitrust law have heretofore operated in their own doctrinal silos,[21] but this pair of developments has led scholars and

[17] In addition to privacy and antitrust law, a third category of platform regulation addresses the speech and content-moderation policies of companies that trade on user-generated expression. *See, e.g.*, Moody v. NetChoice, LLC, 144 S. Ct. 2383, 2393 (2024) (considering whether state laws that restrict social-media platforms' content-moderation violate the First Amendment); Evelyn Douek, *Content Moderation as Systems Thinking*, 136 HARV. L. REV. 526, 531 (2022) (discussing platforms' approaches to content moderation).

[18] *See* Matthew Sipe, *Covering Prying Eyes with an Invisible Hand: Privacy, Antitrust, and the New Brandeis Movement*, 36 HARV. J.L. & TECH. 359, 386-87 (2023).

[19] *See id*. at 386-87.

[20] *See, e.g.*, FTC v. Microsoft Corp., 681 F. Supp. 3d 1069, 1089-90 (N.D. Cal. 2023) (video-game developer acquisition); FTC v. Meta Platforms Inc., 654 F. Supp. 3d 892, 921 (N.D. Cal. 2023) (virtual-reality fitness app acquisition); Complaint at 4, United States v. Google LLC, No. 23-cv-00108 (E.D. Va. Jan. 24, 2023) (digital advertising); Complaint at 2, United States v. Google LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020) (default search-engine agreements). As for why these examples illustrate the Neo-Brandeis movement, see Complaint at 13, 39, United States v. Google LLC, No. 23-cv-00108 (E.D. Va. Jan. 24, 2023) (alleging that Google's conduct has "severely weakened, if not destroyed, competition in the ad tech industry" and that Google has been "happy to exploit its users' privacy when it furthered its own economic interests"); Joseph V. Coniglio, *The Neo-Brandeisian Merger Paradox: A Return to Double Standards*, INFO. TECH. & INNOVATION FOUND. (Nov. 22, 2023), https://itif.org/publications/2023/11/22/the-neo-brandeisian-merger-paradox-a-return-to-double-standards/ [https://perma.cc/PST8-JZD6]; Adrian Wooldridge, *In US Antitrust War, Bet on Brandeis Not Bork*, BLOOMBERG (Mar. 26, 2024, 10:00 PM), https://www.bloomberg.com/opinion/articles/2024-03-27/in-us-antitrust-war-bet-on-brandeis-not-bork [https://perma.cc/UJ9D-FHMH]; *see also infra* notes 135–136 and accompanying text.

[21] Antitrust law has been concerned with consumer welfare, whereas privacy law is part of consumer protection. The divide between consumer welfare and consumer

policymakers to increasingly question how the doctrines interact.[22] To date, these debates have asked what role, if any, privacy should play in the antitrust analysis.[23] Little has been written about the converse — how new privacy rules are shaping the competitive landscape. This Article fills that void by arguing that these new privacy rules tend to benefit large incumbent firms, and it offers a typology that explains how. Specifically, new privacy rules confer three distinct powers on established firms.

First is the power to comply.[24] Large companies comparatively benefit from burdensome regulatory regimes because they have more resources to dedicate to compliance efforts.[25] If regulatory compliance constitutes high fixed costs, new firms will be deterred from entering the market.[26] Privacy rules are not exempt from this microeconomic theory: others have shown how large software companies have borne the regulatory burden of the GDPR relatively easier than their smaller rivals because they have the resources to hire the programmers, lawyers, and technologists necessary to build bespoke compliance regimes in-house, and these compliance efforts exhibit economies of scale.[27] Smaller companies without such resources resort to farming out their compliance efforts to third-party vendors, and they pay a premium for the privilege.[28]

The current approach to privacy law, though, exacerbates this pathology. The most recent crop of omnibus privacy laws relies almost exclusively on the assertion of individual control rights and takes individual consent as the touchstone for the permissible collection and

protection has persisted since the 1931 Supreme Court decision in *Federal Trade Commission v. Raladam Co.* helped spur Congress to supplement the FTC's "unfair methods of competition" authority with authority over "unfair and deceptive acts or practices" in the 1938 Wheeler-Lea Act. *See* Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 457, 462-72 (2021).

[22] *See* discussion *infra* Part II.

[23] *See id.*

[24] *See infra* Part III.1.

[25] *See infra* notes 168–171 and accompanying text.

[26] *See infra* notes 168–169 and accompanying text.

[27] *See infra* notes 179–189 and accompanying text.

[28] *See infra* notes 183–186 and accompanying text.

processing of information.[29] Relying so heavily on individual choice benefits large informational platforms in several ways. For one, they have little trouble obtaining user consent because they have already amassed a deep and wide bench of products and services that few users can imagine foregoing.[30] And for another, consent and rights-assertion mechanisms are simply software features, which are expensive to initially build but can be delivered to an enormous number of users for very low cost.[31] So companies both large and small must build materially identical user-facing software experiences to comply with these privacy laws, but software's low cost of distribution means that large companies amortize the significant upfront investment across a much larger userbase.[32] Privacy law's reliance on software-creation mandates, therefore, provides incumbents with a comparative advantage.

Second is the power to restrict.[33] Another fundamental dynamic is at play here: data has[34] significant financial value at sufficient scale, and thus mandates to share data and extend data flows can be a boon to competition.[35] But mandating increased data access runs counter to most privacy laws, which in theory empower individuals to limit their data-sharing preferences.[36] Opening up dominant platforms' databases for competition purposes, therefore, works against privacy law's user-control paradigm.

At the same time, data has proven remarkably difficult for companies to protect using formal legal processes. Databases of information collected about users have long been understood to lie beyond the

[29] *See infra* Part I.

[30] *See infra* notes 188–190 and accompanying text.

[31] *See infra* note 195 and accompanying text.

[32] *See infra* notes 195–196 and accompanying text.

[33] *See infra* Part III.2.

[34] Here, and throughout this Article, I use *data* as a singular mass noun, rather than as an admittedly more-technically-correct plural count noun. At this point, "few people use it as a plural, yet many know that it is technically a plural," so whichever usage you adopt, "you'll bother some of your readers." BRYAN A. GARNER, GARNER'S MODERN ENGLISH USAGE 245 (4th ed. 2016). Because the mass-noun usage is now ubiquitous, I adopt it here. *See id.*

[35] *See infra* notes 197–207 and accompanying text.

[36] *See infra* notes 205–208 and accompanying text.

protection of intellectual property law.[37] Consent-based privacy laws afford dominant companies a legal tool for shielding their data from competitors that they would otherwise lack. After all, the users consented to collection and processing on terms dictated by the dominant companies, meaning that the dominant firms can self-impose a duty to protect that data against scraping or collection by third parties — including competing firms.[38] So new privacy laws don't just limit regulators' ability to leverage data's equalizing force; they also actively confer on incumbents a novel and potent legal tool for further concealing the source of their financial advantage.

Third is the power to circumvent.[39] One widely remarked-upon feature of rights-based privacy laws is that few people bother exercising those rights.[40] Their net effect, then, is to place a veneer of legitimacy on the vast majority of data collection and processing while leaving a few datapoints missing in the companies' extensive databases. At sufficient scale, those missing datapoints become irrelevant, as illustrated by Apple's Ad Tracking Transparency initiative.[41] Machine-learning and artificial-intelligence advances allow companies with the most data to inferentially fill those gaps — moving from a world of deterministic measurement to an almost-as-good probabilistic one.[42] Since only the largest companies are capable of making such precise and profitable inferences, privacy rules that rely on control rights ensure that dominant incumbents will overcome the lost data while mortally wounding smaller competitors.[43]

These dynamics raise difficult questions for those seeking to rein in the power of dominant informational platforms. If privacy and competition are — in the main, at least — in a zero-sum contest, how should policymakers respond?[44] They may be tempted to select only for

[37] *See infra* notes 225–228 and accompanying text.

[38] *See infra* notes 229–232 and accompanying text.

[39] *See infra* Part III.3.

[40] *See, e.g.*, *infra* note 90 and accompanying text.

[41] *See infra* notes 62–63 and accompanying text.

[42] *See infra* notes 287–288 and accompanying text.

[43] *See infra* note 261 and accompanying text.

[44] There is a vast and rich literature on the proper definition of the term *privacy*. *See, e.g.*, María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social*

competition and eschew privacy, since the Neo-Brandeisians argue that competition produces privacy, but this Article posits that privacy rules can reduce competition. But that would be a grave mistake. There are good reasons to doubt the quality of the privacy that competition produces, and newly competitive markets could just as easily produce new and greater surveillance abuses.[45] And pro-competition policy responses to the powers of incumbency — limiting smaller companies' compliance obligations, opening up data flows, and the like — will themselves undermine privacy rules.[46]

The answer should therefore reside in privacy law — what it is and what we're asking it to do.[47] Scholars have convincingly shown that privacy law's prevailing consent-and-control paradigm produces limited

Taxonomy, 124 COLUM. L. REV. 507 (2024) (discussing the difficulty in defining privacy); Jeffrey Bellin, *Pure Privacy*, 116 NW. U. L. REV. 463 (2021) (proposing a concrete definition of privacy for legal discourse); *see also* sources cited *infra* note 204. In past work, I have advocated in favor of a privacy theory called contextual integrity. *See* Peter Ormerod, *Making Privacy Injuries Concrete*, 79 WASH. & LEE L. REV. 101, 146–50, 176–78 (2022). But here and throughout this Article, I seek to avoid wading into the contested waters of how to best define the term. Rather, for purposes of this Article, I take recent state-level privacy laws at their word — that their aim is to protect consumer privacy by conferring on individuals a series of control rights. *See infra* Part I.1; *see also* Chander et al., *supra* note 14, at 1751 ("The California legislature's articulated intent for the CCPA was to give consumers an effective way to control their personal information by giving them the right to know what personal information is being collected about them and the right to know whether their personal information is sold or disclosed and to whom." (internal quotation marks, brackets, and ellipses omitted)); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 959 (2017) ("[F]or better or worse, the dominant conceptualization of privacy in data protection regimes around the world is control over personal information."). The central contention of this Article, then, is that these privacy laws are ineffective at providing users with meaningful control over their information, *see infra* Part. I.2, and they come at the expense of further advantaging the companies that already dominate digital markets, *see infra* Part III. Privacy laws divorced from the control paradigm stand the best chance of meaningfully disciplining these firms while also protecting a thicker conception of privacy. *See infra* Part IV.2; *see also* Peter Ormerod, *Regulating Data Monetization* (unpublished manuscript) (draft on file).

[45] *See infra* Part IV.1.1.

[46] *See infra* Part IV.1.2.

[47] *See infra* Part IV.2.

benefits,[48] and as this Article shows, it comes at significant cost to other public imperatives. Leveling the playing field while curbing the abuses of the surveillance-profit imperative requires an information-governance regime that speaks directly to how data can and should be used in the public interest. Recent regulatory developments that focus on first-party data, calls for reinvigorating data-use limitations, and proposals that target firms' ability to monetize data all hold promise. Few easy answers are available, but this Article offers policymakers new clarity about the challenges they face.

This Article has four parts. Part I details recent changes to privacy rules and critiques their shared assumptions. Part II surveys the evolution in antitrust scholars' understanding of how privacy and competition interact. Part III offers the typology of the powers of incumbency. In light of these powers, Part IV examines lessons for both antitrust law and privacy law.

I. PRIVACY LAW'S CONSENT-AND-CONTROL PARADIGM

In recent years, governments and companies have enacted and implemented a series of remarkably similar policy changes in the name of protecting digital privacy. This Part first surveys these recent developments and then reviews some shortcomings with their shared approach.

A. Recent Developments

Historically, privacy law comprised sector-specific federal statutes, Federal Trade Commission ("FTC") consent decrees, and a default transparency obligation known as notice-and-choice.[49]

The European Union's implementation of the General Data Protection Regulation ("GDPR") in 2018 set off a cascade of privacy law

[48] *See, e.g.*, Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 597-602 (2021) (surveying scholars' critical accounts); Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/W2GA-E8ZM] ("The continuing optimism about consent-based approaches to privacy governance is mystifying, because the deficiencies of such approaches are well known and relatively intractable.").

[49] Ari Ezra Waldman, *The New Privacy Law*, 55 UC DAVIS L. REV. ONLINE 19, 22 (2021).

changes in the United States.[50] The next month, the California legislature enacted the California Consumer Privacy Act ("CCPA"),[51] and in the years since, GDPR- and CCPA-style privacy laws have proven incredibly influential.[52]

The GDPR revolves around the "lawful processing" of data, which generally requires that personal data may only be processed after a data controller has obtained individual consent.[53] On top of this consent foundation, the law provides European Union internet users a series of additional data-related rights, such as the right to be notified about a security breach, the right to access information, the right to erasure, and the right to data portability, among others.[54] The CCPA adopts a similar structure. Like the GDPR, it defines personal information broadly, emphasizes transparency, and it includes notice, access, portability, and opt-out rights.[55]

California voters also approved a ballot initiative — the California Privacy Rights Act — in 2020 to expand and refine aspects of the CCPA.[56] More states have since followed California's lead. In 2021 and 2022, Virginia, Colorado, Utah, and Connecticut enacted new privacy laws modeled on the CCPA.[57] In 2023, an additional seven states passed

[50] *See id*. at 21.

[51] *See* Wakabayashi, *supra* note 12.

[52] *See* Waldman, *supra* note 49, at 21-22.

[53] *See* Chander et al., *supra* note 14, at 1756 (citing GDPR, art. 6(1)(a)). In addition to individual consent, the GDPR enumerates five other categories of lawful processing. *See id*. (citing GDPR, art. 6(1)(a)–(f)).

[54] *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1908-09 (2019) (citing GDPR, arts. 15–18, 20–21, 33).

[55] *See* Chander et al., *supra* note 14, at 1746-53.

[56] *See California Consumer Privacy Laws*, BLOOMBERG L., http://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ (last visited July 22, 2024) [https://perma.cc/V43A-XK8S].

[57] *See* Taylor Kay Lively, *Connecticut Enacts Comprehensive Consumer Data Privacy Law*, IAPP (May 11, 2022), http://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law/ [https://perma.cc/NR5V-WRVB]; Taylor Kay Lively, *Utah Becomes Fourth US State to Enact Comprehensive Consumer Privacy Legislation*, IAPP (Mar. 25, 2022), http://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/ [https://perma.cc/EZ2Z-96JF]; Sarah Rippy, *Colorado Privacy Act Becomes Law*, IAPP (July 8, 2021), http://iapp.org/news/a/colorado-privacy-act-becomes-law/ [https://perma.cc/7ALF-92CZ]; Sarah Rippy, *Virginia Passes the*

similar laws, with seven more enacted in 2024.[58] Many other states have been or are actively considering CCPA-style privacy laws.[59] Meanwhile, Congressional negotiators have coalesced around a federal proposal that would adopt the CCPA's consent-and-control framework, while simultaneously preempting all state-law efforts.[60]

This shared approach to privacy has not been limited to public policy. Several large technology companies have undertaken initiatives that take cues from the GDPR and CCPA. Most significant is Apple's App Tracking Transparency ("ATT") initiative.[61] First announced in June 2020 and implemented in April 2021, ATT requires applications — as a condition of remaining in some of Apple's various App Stores — to obtain opt-in user consent to cross-site and -app tracking.[62] Before ATT was implemented, users could choose to opt out of tracking; ATT switched the default state, requiring apps to obtain permission before tracking users.[63] By some estimates, switching the default from opt-out to opt-in decreased the percentage of users who allowed tracking from about seventy-five percent to about twenty percent.[64] Google has

Consumer Data Protection Act, IAPP (Mar. 3, 2021), http://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/ [https://perma.cc/4N29-D6X4].

[58] *See* Folks, *supra* note 16.

[59] *See id.*

[60] *See* Peter Swire, *The Bipartisan, Bicameral Privacy Proposal Is a Big Deal*, LAWFARE (June 9, 2022, 2:12 PM), https://www.lawfaremedia.org/article/bipartisan-bicameral-privacy-proposal-big-deal [https://perm5a.cc/EJ4G-5K8S].

[61] *See infra* notes 62–63 and accompanying text.

[62] *See* Brian X. Chen, *Apple Announces New Privacy Features*, N.Y. TIMES (June 23, 2020), http://nytimes.com/2020/06/23/technology/apple-announces-new-privacy-features.html; Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice.*, N.Y. TIMES (Sept. 29, 2021), http://nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html; *see also User Privacy and Data Use*, APPLE, http://developer.apple.com/app-store/user-privacy-and-data-use/ (last visited July 14, 2024) [https://perma.cc/98GR-N6T3]; *App Review Guidelines* §§ 3.2.2(vii), 5.1.2(i), APPLE, http://developer.apple.com/app-store/review/guidelines/ (last updated June 10, 2024) [https://perma.cc/8F3J-NU29].

[63] *See* Thorin Klosowski, *Looking Back on a Year of Apple's Privacy Labels and Tracking*, N.Y. TIMES (Mar. 31, 2022), http://nytimes.com/wirecutter/blog/apple-privacy-labels-tracking/.

[64] *See id.*

announced plans to implement a similar feature on Android.[65] Google has also recently scrapped its long-running effort to eliminate third-party cookies in Chrome and is now pursuing a consent-based approach that resembles ATT.[66]

B. Shortcomings

Privacy law's prevailing paradigm purports to offer users the ability to control their personal information. But the new omnibus laws surveyed above fall short of this objective for at least two independent reasons.

Older privacy laws, the CCPA, and their lookalike follow-ons are all "pervasively informed by a governance paradigm that is deeply embedded in the U.S. legal tradition and that relies on individual assertion of rights to achieve social goals."[67] Within this paradigm, "individual control rights function as the primary mechanism for governing the collection and processing of personal data, with no or only residual provision for ongoing governance at the collective level."[68]

---

[65] *See* Anthony Chavez, *Introducing the Privacy Sandbox on Android*, GOOGLE: THE KEYWORD (Feb. 16, 2022), http://blog.google/products/android/introducing-privacy-sandbox-android/ [https://perma.cc/4F82-ZT9Y].

[66] *Prepare for phasing out third-party cookies*, GOOGLE, developers.google.com/privacy-sandbox/3pcd (last visited July 14, 2024) [https://perma.cc/V4VX-6NRJ]; *see also* Richard Lawler, *Google's Turning Off Third-Party Cookies for 1 Percent of Chrome Users Early Next Year*, THE VERGE (May 18, 2023, 8:19 AM), theverge.com/2023/5/18/23728263/google-chrome-ad-tracking-third-party-cookies-privacy-sandbox [https://perma.cc/GQ69-4FE7] ("Google has been talking about a plan for Chrome to block the third-party cookies that can track user activity across many different websites since 2020. . . . Three years later, it hasn't happened, as its proposals for replacement technology have been criticized by competitors and privacy advocates and scrutinized by regulators who want to know if they will give Google an unfair advertising advantage."); Richard Lawler, *Google's Plan to Turn Off Third-Party Cookies in Chrome is Dying*, THE VERGE (July 22, 2024), https://www.theverge.com/2024/7/22/24203893/google-cookie-tracking-prompt-ad-targeting-privacy-sandbox [https://perma.cc/9YCX-6B6Z] ("Now, Chrome will ask users to 'make an informed choice that applies across their web browsing' instead of deprecating third-party cookies, writes Google Privacy Sandbox VP Anthony Chavez. That could work more like Apple's app tracking opt-in, a setting that reportedly cost social media platforms nearly $10 billion when it rolled out in 2021.").

[67] Cohen, *supra* note 48, at 3.

[68] *Id.* at 4.

There are good reasons to doubt the efficacy of this consent-and-control paradigm.[69] At a fundamental level, when we reveal information about ourselves, we necessarily also reveal information about others in unpredictable and inscrutable ways. Companies' use of massive databases to make precise and profitable inferences about human behavior therefore undermines the very idea of withholding consent.[70] Contemporary "information privacy protections do not grapple with the way that machine learning facilitates an inference economy in which organizations use available data collected from individuals to generate further information about both those individuals and about other people."[71] Consent-and-control privacy laws are a poor fit in a world where seemingly innocuous data — analyzed at scale — can unlock profitable insights.[72]

The laws that govern data today, in other words, have a sociality problem: by focusing on individual rights and harms, the prevailing paradigm fails to recognize that data's value comes from relating people to one another — "how we are alike biologically, interpersonally, politically, and economically."[73] In today's information economy, companies routinely use population-level databases for behavioral profiling, targeted advertising, prediction tasks, and large-scale risk assessment "to predict and change behavior, to gain intimate consumer or competitor knowledge for market advantage, and to retain greater surplus value."[74]

---

[69] *See, e.g.*, *id.* ("The continued optimism about consent-based approaches to privacy governance is mystifying, because the deficiencies of such approaches are well known and relatively intractable.").

[70] *See, e.g.*, Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 63 (Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, eds., 2014) ("So long as a data collector can overcome sampling bias with a relatively small proportion of the consenting population, this minority will determine the range of what can be inferred for the majority").

[71] Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022).

[72] *Id.* at 423.

[73] Viljoen, *supra* note 48, at 608-09.

[74] *Id.* at 610.

To illustrate the dynamic, consider a retailer that sought to reduce its exposure to customers defaulting on their credit cards by identifying signals that correlated with credit risk.[75] Using a massive database of existing card holders, their purchase histories, and whether they had previously defaulted, the retailer found that customers who had purchased furniture anti-scuff pads rarely defaulted, while customers who frequented pool halls posed an outsized credit risk.[76] The company then used these and similar insights to inform its future credit decisions.[77] We are constantly revealing not just information about ourselves but also about people we will never meet who are similar and dissimilar from us in ways both large and small. Each of us has little reason to jealously guard such information, but companies realize significant surplus value from collecting such data and wringing predictive insights out of it at scale.

Relying on individual control rights thus creates a structural mismatch in the relationship between individuals and data collectors: individuals have only a fractional interest in a particular data flow, while data collectors have every motivation to collect as much data as possible.[78] The value of population-level data means that "one's actions in the data political economy necessarily impact others in uneven ways over which one has no direct control."[79]

A second problem concerns the malleability of consent. Software affords companies an unparalleled opportunity to stack the deck in their favor by manipulating the environment in which consent is obtained.[80] Researchers have empirically shown how companies easily exploit people's instinct to trust the perceived benevolence of a putative data

[75] *See* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in The Age of Predictive Analytics*, 79 MD. L. REV. 439, 453-54 (2020) (discussing Dana Flavelle, *What the Data Crunchers Know About You*, TORONTO STAR (Apr. 23, 2010), thestar.com/business/technology/what-the-data-crunchers-know-about-you/article_aeec4493-55cf-5340-80e0-3e96005b49bb.html [https://perma.cc/Z743-2JRV]).

[76] *Id.*

[77] *Id.*

[78] Viljoen, *supra* note 48, at 612-13.

[79] *Id.* at 653.

[80] *See infra* notes 77–82 and accompanying text. *See supra* notes 77–79 and accompanying text; *see infra* notes 81–82.

collector that seeks their consent.[81] The researchers hypothesized that people use a simple and easy-to-manipulate trust heuristic when making decisions that involve the disclosure of personal information: that we are more willing to trust and disclose information when a data collector signals its benevolence.[82] By way of illustration, the researchers offered their subjects two ways to obtain payment: an anonymous cash pickup and a disclosure-heavy bank transfer.[83] When the subjects were told that a privacy rule required the researchers to offer subjects the anonymous option, the subjects were far more likely to elect it.[84] When instead the subjects were led to believe the anonymous option was being offered by the good grace of the experimenters, the subjects were more likely to trust them and share their banking details.[85] The researchers' findings further showed the trust heuristic tends to override and crowd out other credible information about the collector's intentions.[86]

Companies seeking consent to collect information can thus easily design software experiences that maximize disclosure by simply providing "cheap choice options" or by making "misleading statements about their own intentions or practices to induce trust in consumers."[87] The widespread use of A/B testing further allows companies to sharpen and refine their data extraction prompts for maximum efficiency.[88]

These two shortcomings work together to ensure that privacy laws don't accomplish very much: data collectors have every ability to manipulate users into granting consent to collect and process information, and the users have no meaningful information about what consent entails. For the companies, the data's value extends far beyond the sum of its parts, rendering legible even those users who withhold

[81] Christopher Jon Sprigman & Stephan Tontrup, *Privacy Decisions Are Not Private: How the Notice and Choice Regime Induces Us to Ignore Collective Privacy Risks and What Regulation Should Do About It*, No. 23-22 N.Y.U. L. ECON. RSCH. (2023).

[82] *See id.* at 11-14.

[83] *See id.* at 5-6, 15-21.

[84] *Id.*

[85] *Id.*

[86] *See id.* at 40.

[87] *Id.* at 46-47.

[88] *See, e.g.*, Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM, at 297-300 (discussing Google's and Facebook's use of A/B testing).

consent.[89] Despite the charade, industry and their political allies insist that users are "empowered" to exercise agency over their information, no matter how burdensome it is to exercise those rights and no matter how obscure the benefits of doing so.[90]

***

Recent years have witnessed a spate of new privacy laws on both sides of the Atlantic. These laws operate principally through the assertion of individual control rights and place particular emphasis on consent. As privacy considerations have moved to the fore of public debate about large informational platforms, antitrust scholars have increasingly questioned how competition and privacy both do and should interact. The next Part surveys scholars' attempts to understand their interaction.

II. PRIVACY'S ROLE IN ANTITRUST LAW

As new privacy laws have been proposed, enacted, and implemented, digital markets have been dominated by a few large firms. In the past eight years, Google Search has consistently owned over eighty percent of the search engine market,[91] and Google's apps own an even larger share of the domestic market for mapping services.[92] In 2022, just three companies — Google, Meta, and Amazon — generated over sixty percent of all digital advertising revenue in the United States.[93] Nearly every other person on the planet uses one or more of Meta's products

[89] *See* Barocas & Nissenbaum, *supra* note 70.

[90] *See* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 984-93 (2023).

[91] *See* Bianchi, *supra* note 4.

[92] *See* Laura Ceci, *Most Popular Mapping Apps in the United States as of April 2018, by reach*, STATISTA (Aug. 25, 2023), statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/ [https://perma.cc/4X5X-LFES].

[93] *See Share of Ad-Selling Companies in Digital Advertising Revenue in the United States from 2020 to 2025*, STATISTA (May 30, 2023), statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/ [https://perma.cc/45Y7-CNZD].

on a monthly basis,[94] and Amazon's share of retail e-commerce is six times the size of its closest competitor.[95] Globally, Apple and Microsoft control about ninety percent of the desktop operating system market, while Apple and Google control over ninety-*nine* percent of the mobile operating system market.[96] Americans ultimately spend on average over eight hours a day consuming digital media on those devices.[97]

Antitrust scholars and policymakers have unsurprisingly come to question the forces driving such high levels of digital-market concentration.[98] Since so many digital products and services are either partially or fully subsidized by advertising, grasping how companies collect, process, and monetize user data is essential to understanding the forces shaping digital markets. And how companies collect, process, and monetize user data inevitably involves questions about privacy policies and regulations. Over the past decade, scholars and policymakers have therefore increasingly debated the ways that privacy law and competition law interact in digital markets. There are three dominant approaches to theorizing this interaction: separation, integration, and tension. This Part surveys them.

---

[94] *See* Stacy Jo Dixon, *Cumulative Number of Monthly Meta Product Users as of 2nd Quarter 2023*, STATISTA (July 27, 2023), statista.com/statistics/947869/facebook-product-mau/ [https://perma.cc/67BB-B82D].

[95] *See* Stephanie Chevalier, *Market Share of Leading Retail E-Commerce Companies in the United States as of June 2022*, STATISTA (July 10, 2023), statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/ [https://perma.cc/ZXM7-W454].

[96] *See Global Market Share Held by Operating Systems for Desktop PCs, from January 2013 to July 2023*, STATISTA (Sept. 3, 2023), statista.com/statistics/218089/global-market-share-of-windows-7/ [https://perma.cc/Z74M-4V99]; *Global Market Share Held by Mobile Operating Systems from 1st Quarter 2009 to 2nd Quarter 2023*, STATISTA (Aug. 31, 2023), statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ [https://perma.cc/P8QN-K355].

[97] *See* A. Guttmann, *Average Time Spent Per Day With Digital Media in the United States From 2011 to 2024*, STATISTA (July 10, 2023), statista.com/statistics/262340/daily-time-spent-with-digital-media-according-to-us-consumsers/ [https://perma.cc/DVJ5-DT9W].

[98] *See, e.g.*, John M. Newman, *Antitrust in Digital Markets*, 72 VAND. L. REV. 1497 (2019) (investigating how and why digital markets produce uniquely durable market power).

A. Separation

The first approach regards privacy law and antitrust law as distinct doctrinal silos that do not — and should not — have anything to do with one another.

There is effectively no scholarly discussion of the two doctrines' interaction before the twenty-first century. This may initially seem surprising, but the void makes sense within view of each doctrine's genealogy. Antitrust law in the United States traces its origins to the Gilded Age and the passage of the Sherman Act in 1890.[99] Beginning in the 1960s, however, the neoclassical Chicago School began waging a concerted campaign to constrain antitrust enforcement.[100] Those efforts were wildly successful, culminating around the turn of the millennium in "the anti-monopoly provisions of the Sherman Act [going] into a deep freeze from which they have never really recovered."[101]

Information privacy law is of a considerably younger vintage. The Fair Credit Reporting Act, initially enacted in 1970, is the first federal consumer privacy law and one of the first in the world.[102] Even after its enactment, privacy law remained isolated to a few distinct realms like credit reporting, telecommunications, and health and financial information.[103] Only in the late 1990s did the FTC begin enforcing the promises contained in companies' privacy policies as part of its consumer-protection mandate.[104] Just a decade ago, two leading privacy scholars noted that the FTC's approach — the primary regulation of

[99] *See generally* Sanjukta Paul, *Recovering the Moral Economy Foundations of the Sherman Act*, 131 YALE L.J. 175, 181 (2021) (documenting the "moral economy" origins of antitrust and the common law of restraint of trade).

[100] *See* Lina Khan & Sandeep Vaheesan, *Market Power and Inequality: The Antitrust Counterrevolution and Its Discontents*, 11 HARV. L. & POL'Y REV. 235, 236-38 (2017).

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

[102] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 270 (2016).

[103] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

[104] *See id.* at 585 ("Since the late 1990s, the Federal Trade Commission . . . has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices.")

privacy in the United States — had mostly escaped scholarly study.[105] The rise of information privacy law thus coincided with a multi-decade dearth of monopolization enforcement by domestic antitrust authorities.[106] Until recently, privacy and competition law had passed one another like two ships in the night.

The business model of large informational platforms is also an ideal fit for evading scrutiny under the Chicago School. The paradigmatic digital business model constitutes "giving a product away for free . . . in order to collect data that can be used for lucrative targeted advertising."[107] Since the Chicago School focuses singularly on supra-competitive prices as a proxy for consumer welfare,[108] digital businesses that don't charge users a price other than surveillance have traditionally escaped antitrust scrutiny.[109]

Neoclassical economists' singular focus on market efficiency pervades the work of the first scholars to contemplate the privacy and antitrust interaction. James C. Cooper, for example, argued in 2013 that allowing antitrust enforcement to consider privacy would "inject an undesirable level of subjectivity into antitrust enforcement decisions," thereby attracting "socially wasteful rent-seeking expenditures and . . . deter[ing] beneficial data collection efforts."[110] Ultimately, he

[105] *Id.* at 585-86.

[106] Erika M. Douglas, *The New Antitrust/Data Privacy Interface*, 130 YALE L.J. F. 647, 652 (2021) [hereinafter Douglas, *Interface*].

[107] Matt Levine, *Elon Musk Isn't Getting Enough Sleep*, BLOOMBERG: MONEY STUFF (Jan. 8, 2024, 11:28 AM), bloomberg.com/opinion/articles/2024-01-08/elon-musk-isn-t-getting-enough-sleep [https://perma.cc/8WFR-SD3K].

[108] *See, e.g.*, Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 719 (2017) (quoting Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 933 (1979)).

[109] *See, e.g.*, Julie E. Cohen, *Law for the Platform Economy*, 51 UC DAVIS L. REV. 133, 189 (2017) ("A final group of problems involves platform conduct that is simply intractable using conventional regulatory methodologies. Debates about the need for antitrust oversight of platform-based environments are one example. . . . Because platforms can define terms for each user group separately, pricing is not a reliable sign of market power in two-sided markets . . . .").

[110] James C. Cooper, *Privacy & Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1129 (2013).

concluded, "antitrust is the wrong vehicle to address privacy concerns."[111]

Two years later, then-FTC Commissioner Maureen K. Ohlhausen and her attorney-advisor coauthor echoed Cooper's concerns.[112] Reflecting on the FTC's dual roles in policing consumer protection and competition, they argued that the "commingling of the competition and consumer protection laws . . . is unnecessary and could lead to confusion and doctrinal issues in antitrust, without true gains to consumer protection."[113] Emphasizing that the two doctrines were — in their view — complementary, they claimed that competition laws "are not designed to address conduct that may be unjust or immoral, unless it also happens to harm competition."[114] Ultimately, they concluded that attempts "to unify the competition and consumer protection laws creates needless risks for the Internet economy and could destabilize the modern consensus on antitrust analysis, again pulling it away from rigorous, scientific methods developed in the last few decades."[115]

Competition authorities' policy decisions at the time reflected this consensus. In the early-to-mid 2010s, competition policymakers globally shared a set of assumptions about digital markets, including that privacy laws and competition laws serve different ends; market forces would solve many privacy issues; and that data offered few, if any, competitive advantages.[116] Because these beliefs were widely shared, competition authorities allowed the dominant informational platforms to acquire hundreds of companies — authorities rarely bothered to investigate mergers, and none were blocked.[117]

As the last decade wore on, however, policymakers and scholars began questioning whether consumer welfare and consumer protection always resided on parallel tracks.

---

[111] *Id.* at 1146.

[112] Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right [*Approach*] to Privacy, 80 ANTITRUST L.J. 121, 153-54 (2015).

[113] *Id.* at 138.

[114] *Id.* at 147.

[115] *Id.* at 160.

[116] *See* Maurice E. Stucke, *The Relationship Between Privacy and Antitrust*, 97 NOTRE DAME L. REV. REFLECTION 400, 401-02 (2021).

[117] *Id.* at 402.

B. Integration

The second approach seeks to integrate privacy considerations into the antitrust analysis.

The integrationist movement is part of a broader effort to reclaim antitrust law from the neoclassical Chicago School.[118] Whereas the prevailing Chicago School approach focuses singularly on consumer welfare — and more specifically, on supra-competitive prices — the Neo-Brandeis movement takes a broader view. The Neo-Brandeis movement departs from the Chicago School's consumer-welfare focus in two salient ways: it is inherently skeptical of concentrated economic power, and it urges policymakers to consider broader social and political goals in the antitrust analysis.[119]

Integrationists posit that privacy is a non-price parameter akin to product quality.[120] The head of the Department of Justice's Antitrust Division in 2019 explained: "[D]iminished quality is also a type of harm to competition. As an example, privacy can be an important dimension of quality. By protecting competition, we can have an impact on privacy and data protection. Moreover, two companies can compete to expand privacy protections for products or services."[121] One commonly cited illustration of integrationist theory is DuckDuckGo.[122] The company offers a search engine that, in contrast to Google's, does not collect personal data, and its marketing efforts emphasize its privacy-protecting bonafides.[123]

---

[118] *See generally* Sipe, *supra* note 18 (articulating the principles of the Neo-Brandeis movement).

[119] *See id.* at 388.

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

[121] Markan Delrahim, Assistant Attorney General, DOJ, Remarks for the Antitrust New Frontiers Conference (June 11, 2019), justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers [https://perma.cc/7F2E-5VNR].

[122] *See, e.g.*, Sammi Chen, *The Latest Interface: Using Data Privacy as a Sword and Shield in Antitrust Litigation*, 74 HASTINGS L.J. 551, 565 (2023) (citing DuckDuckGo as an illustration of integrationists' "privacy as quality" theory).

[123] *See id.* It turns out, however, that DuckDuckGo is not nearly as privacy-protecting as the company would like you to believe. *See* Andy Greenberg, *Security News This Week: DuckDuckGo Isn't as Private as You Think*, WIRED (May 28, 2022, 9:00 AM),

Casting privacy as a non-price parameter has several related implications. First, it suggests that competitive markets will produce greater privacy protections than monopolistic or oligopolistic markets.[124] For example, Dina Srinivasan has argued that Facebook initially competed "in a contested market with superior representations of protecting consumer privacy, including the specific promise not to track and monitor consumers' digital footprints."[125] Facebook added the condition of surveillance to its mandatory terms only after rivals exited and it came to dominate social networking.[126]

Second, it requires that antitrust analyses — of both mergers and domination — contemplate the effects on privacy-based competition.[127] Within the merger context, integrationists have harshly criticized Facebook's acquisition of WhatsApp.[128] Before the acquisition, privacy was a critical site of nonprice competition.[129] Facebook's Messenger service was free but — in service to its advertising-based business — collected a vast array of personal information, whereas WhatsApp charged a nominal fee and promised to collect only its users' mobile phone numbers.[130] Just a couple years after the merger, WhatsApp made a "dramatic privacy about-face," updating its terms and conditions to

https://www.wired.com/story/duckduckgo-microsoft-twitter-ft-bush-assassination-whatsapp/ [https://perma.cc/JRD2-HKBY].

[124] *See* Douglas, *Interface*, *supra* note 106, at 655-56 ("[I]ntegrationist theory considers whether a transaction is likely to lessen pressure on the merging firms to compete based on privacy, resulting in fewer privacy-protective product options for consumers post-merger. This reflects a relationship where competition drives privacy, and when one declines, so does the other."); Stucke, *supra* note 116, at 406 ("Basically, competition and privacy were seen as complementary. With more competition, firms will be more responsive to our privacy interests.").

[125] Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERK. BUS. L.J. 39, 44 (2019).

[126] *Id.* at 44-45.

[127] *See* Douglas, *Remedies*, *supra* note 120, at 27-29.

[128] *See, e.g.*, Stucke, *supra* note 116, at 402-03 ("None of the competition agencies challenged the transaction, but the European Commission published an opinion explaining its rationale. . . . [T]he Commission's analysis of the merger was woefully deficient.").

[129] *See id.*

[130] *Id.*

allow the sharing of data between it and Facebook.[131] Consolidation, in other words, reduced consumers' privacy offerings and thereby degraded the quality of available services.[132]

Integrationists have also argued that competing on privacy is relevant to monopolization cases. Srinivasan's analysis of Facebook's evolution is one example.[133] Another is the Department of Justice's monopolization suit against Google's domination of the search and search-advertising markets.[134] The district court held that Google's payment of an estimated $20 billion to Apple each year so that Google remains the iPhone's default search engine violates the Sherman Act.[135] The DOJ's complaint explicitly incorporated the integrationist approach: Google's privacy practices are inferior, but its size enables it to pay sums that privacy-protecting alternatives cannot afford.[136] By allowing these default-search arrangements, the theory goes, consumer privacy suffers.[137]

The integrationist approach "is the most developed and accepted view on the interaction between antitrust law and data privacy."[138] It has been cited in merger decisions by the FTC, the Department of Justice, and

[131] *See* Natasha Lomas, *WhatsApp's Privacy U-turn on Sharing Data With Facebook Draws More Heat in Europe*, TECHCRUNCH (Sept. 30, 2016, 6:56 AM), techcrunch.com/2016/09/30/whatsapps-privacy-u-turn-on-sharing-data-with-facebook-draws-more-heat-in-europe [https://perma.cc/5784-H555].

[132] *See also* Reuben Binns & Elettra Bietti, *Dissolving Privacy, One Merger at a Time: Competition, Data, and Third Party Tracking*, 36 COMPUT. L. & SEC. REV. 1, 23-36 (2020), https://ssrn.com/abstract=3269473 [https://perma.cc/CY4V-XBEB].

[133] *See* Srinivasan, *supra* note 125.

[134] *See, e.g.*, Chen, *supra* note 122, at 565-66 (citing Press Release, U.S. Dep't Just., Justice Department Sues Monopolist Google for Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws [https://perma.cc/XC2T-37AT].

[135] *See* United States of America v. Google LLC, 2024 WL 3647498 (D.D.C. Aug. 5, 2024); Casey Newton, *Google Goes to Court*, PLATFORMER (Sept. 7, 2023), platformer.news/p/google-goes-to-court [https://perma.cc/S3NM-GWVN].

[136] *See* Complaint at ¶¶ 149, 167, United States et al. v. Google, LLC, No. 20-cv-03010 (D.D.C. Oct. 20, 2020).

[137] *See id.* As of this writing, the district court has only ruled on the question of liability under the Sherman Act and has not yet addressed the question of remedies. *See* Tim Wu, *What Should We Do About Google?*, N.Y. TIMES (Aug. 13, 2024), https://www.nytimes.com/2024/08/13/opinion/google-antitrust-remedy.html.

[138] Douglas, *Interface*, *supra* note 106, at 655.

European competition authorities,[139] and the Department of Justice's most consequential monopoly enforcement suit in a generation cites privacy harms as a chief anticompetitive effect.[140] The integrationist approach also has support among antitrust scholars.[141]

In sum, recent years have witnessed an evolution in consensus about the relationship between competition and privacy from separation to integration.

C. Tension

Most recently, some scholars have argued that privacy and competition may sometimes be in tension with one another. This third approach marks a departure from the separatists (who view privacy and competition as distinct but complementary) and from the integrationists (who view competition as furthering privacy protections).

Erika M. Douglas has documented the tensions between privacy and competition.[142] Two recent cases illustrate her findings. The first is litigation between LinkedIn and hiQ Labs.[143] hiQ Labs scraped data from LinkedIn users' social networking profiles to use in its "people analytics" software, which promises to alert employers about which of their employees are at risk of resigning.[144] LinkedIn initially permitted

---

[139] *See id*. nn.31–35.

[140] *See* David McCabe & Cecilia Kang, *In Its First Monopoly Trial of Modern Internet Era, U.S. Sets Sights on Google*, N.Y. TIMES (Sept. 6, 2023), nytimes.com/2023/09/06/technology/modern-internet-first-monopoly-trial-us-google-dominance.html; *see also supra* text accompanying note 20.

[141] *See, e.g.*, Douglas, *Interface*, *supra* note 106, at 655 n.35 (citing scholars); Samson Esayas, *Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers*, UNIV. OF OSLO FAC. OF L. RSCH. PAPER NO. 2018-26 (2018). None of this should suggest, however, that the most outspoken separatists have acceded to the integrationists' approach — the debate rages on. *See, e.g.*, James C. Cooper & John M. Yun, *Antitrust & Privacy: It's Complicated*, 2022 U. ILL. J. L., TECH. & POL'Y 343 (2022).

[142] *See* Douglas, *Interface*, *supra* note 106; Douglas, *Remedies*, supra note 120; Erika M. Douglas, *Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis*, 97 NOTRE DAME L. REV. REFLECTION 430 (2022) [hereinafter Douglas, *Justification*].

[143] *See* Douglas, *Interface*, *supra* note 106, at 649-50, 662-64.

[144] *See* hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1185-87 (9th Cir. 2022).

hiQ's scraping, but around the same time that LinkedIn launched a competing software product, LinkedIn took measures to block hiQ's scraping.[145] In response, hiQ brought suit against LinkedIn, alleging a litany of tort, contract, computer-trespass, intellectual-property, and antitrust claims.[146] LinkedIn defended by citing, among other legal defenses, the need to protect its users' privacy.[147] By default, LinkedIn broadcasts when users make changes to their profiles, but it provides a "Do Not Broadcast" setting to allow users to turn off these default announcements.[148] hiQ's software alerted employers to users' profile changes even if they had engaged the "Do Not Broadcast" setting.[149] LinkedIn seized on this facet of hiQ's software to argue that blocking the scraping was necessary to honor LinkedIn users' privacy preferences.[150]

Douglas highlights the palpable tension between privacy and competition at issue in the case: LinkedIn argued it was merely protecting user privacy when it cut off a rival's access to data they were both seeking to monetize. By pitting claims of anticompetitive conduct against an asserted privacy justification, *hiQ v. LinkedIn* shows that privacy and competition can be substitutes, rather than complements.[151]

The second is the litigation between Apple and Epic Games.[152] The case arose when Epic, the developer of the video game Fortnite, offered iOS players a discounted payment alternative to Apple's In-App Purchases — a violation of the iOS App Store rules.[153] After Apple removed Fortnite from the App Store, Epic initiated suit against Apple, alleging antitrust claims under state and federal law.[154] The district court ultimately held that even though Apple's App Store rules had prima facie

[145] *See id.*

[146] *Id.* at 1188.

[147] *See id.* at 1185-86, 1189-90.

[148] *Id.* at 1185-86.

[149] *See* Reply Brief for Defendant-Appellant at 15, hiQ Labs, Inc. v. LinkedIn Corp., No. 17-16783 (9th Cir. Dec. 11, 2017).

[150] *See id.* at 28; Opening Brief for Defendant-Appellant at 59-60, hiQ Labs, Inc. v. LinkedIn Corp., No. 17–16783 (9th Cir. Oct. 3, 2017).

[151] *See* Douglas, *Interface*, *supra* note 106, at 662; *see also* Chen, *supra* note 122, at 568-72.

[152] *See* Douglas, *Justification*, *supra* note 142.

[153] *See* Epic Games, Inc. v. Apple, Inc., 67 F.4th 946, 966-69 (9th Cir. 2023).

[154] *Id.*

anticompetitive effects, Apple had established privacy- and security-related justifications for its anticompetitive conduct.[155] The Ninth Circuit later affirmed this portion of the district court's opinion.[156]

Douglas notes that *Epic v. Apple* similarly illustrates the latent tension between privacy and competition: just like LinkedIn, Apple engaged in anticompetitive conduct and sought to justify doing so on privacy grounds.[157]

Douglas isn't alone. Matthew Sipe has argued that the Neo-Brandeis movement's efforts to improve privacy through competition are likely to prove self-defeating.[158] He contends that increasing competition will not necessarily produce greater privacy protections, and in fact may do the exact opposite. He also argues it will increase uncertainty and vagueness in the application of antitrust law, and it will produce an inequitable distribution of greater privacy protections.[159] Maurice E. Stucke has also argued that there is a looming divide between privacy and competition.[160] Stucke concedes that privacy and competition can be complementary but contends that "more competition will not necessarily improve privacy, especially when the competition itself is toxic."[161]

Despite these divisions over the interaction between privacy and competition, there is broad consensus between integration scholars and tension scholars that competitive concerns preempt privacy considerations.[162] The integrationist approach explicitly "treats data privacy as a factor to be subsumed into existing antitrust understanding."[163] Even those who recognize the tension assume the

---

[155] Epic Games, Inc. v. Apple, Inc., 559 F. Supp. 3d 898, 1002-08, 1038-40 (N.D. Cal. 2022), *aff'd in part & rev'd in part*, 67 F.4th 946 (9th Cir. 2023), *cert. denied*, 144 S. Ct. 682 (2024).

[156] *Epic Games*, 67 F.4th at 966.

[157] *See* Douglas, *Justification*, *supra* note 142, at 432; *see also* Chen, *supra* note 122, at 572-74.

[158] *See* Sipe, *supra* note 18, at 389-417.

[159] *See id.*

[160] *See* Stucke, *supra* note 116; MAURICE E. STUCKE, BREAKING AWAY: HOW TO REGAIN CONTROL OVER OUR DATA, PRIVACY, AND AUTONOMY (2022).

[161] Stucke, *supra* note 116, at 410.

[162] *See supra* notes 154–156.

[163] Douglas, *Interface*, *supra* note 106, at 679.

supremacy of antitrust both descriptively (that regulators do and will prefer competition to privacy when the two conflict)[164] and normatively (that regulators and courts should reject firms' privacy-protecting justifications for conduct that harms competition).[165]

The tension scholars are onto something significant. How antitrust authorities should respond to privacy-related justifications for anticompetitive conduct is surely of keen interest to antitrust doctrine. But the stakes of their interaction are in fact considerably higher than is suggested by this deep-in-the-weeds framing. If we accept that privacy and competition are on a collision path, larger questions loom. Perhaps most significant for those concerned with the wealth and power of large informational platforms is the effect that new privacy laws are having on digital-market competition. Are privacy rules — as is often billed and assumed — restraining the power and reach of technology giants, or is something else going on?

III. THE POWERS OF INCUMBENCY

Despite a lively debate among antitrust scholars about what role, if any, privacy should play in the antitrust analysis, little has been written about the converse: how do privacy laws shape the competitive landscape? This Part fills that void by identifying three distinct powers that the current crop of privacy laws confers on incumbent firms.

A. The Power to Comply

The first is the power to comply. Regulatory mandates of any kind are most easily borne by established firms. This core dynamic is not unique to digital markets or informational platforms but is instead a byproduct of any regulatory regime that imposes significant compliance costs on the regulated industry.[166] Yet the realities of digital markets suggest that incumbents are uniquely positioned to obtain consent to collect and

[164] *See id*. at 679-80.

[165] *See* Douglas, *Justification*, *supra* note 142, at 457-65; *see also* Sipe, *supra* note 18, at 399-414 (arguing that the integrationist approach will harm markets and antitrust doctrine).

[166] *See supra* notes 157–161.

process user data.[167] In other words, while all regulatory mandates are susceptible to advantaging established firms, contemporary privacy laws exaggerate incumbency's benefits.

For decades, competition scholars and policymakers have recognized that regulatory burdens can have a disparate effect. A study of regulatory reform in British Columbia, for example, concluded that a reduction in entry regulations coincided with a surge in new business incorporations.[168] A comparative study of entry regulations in Italy and the United Kingdom similarly found that high entry costs reduced the amount of competition that large incumbent firms faced.[169] Other researchers have reached similar conclusions.[170] Domestically, the Congressional Research Service has noted within the context of financial markets that "the costs of regulatory compliance . . . may impose a barrier to entry that favors incumbents and reduces competition."[171] Likewise, empirical research has shown that

[167] *See infra* notes 177–185.

[168] *See* Laura Jones, *Cutting Red Tape in Canada: A Regulatory Reform Model for the United States?*, MERCATUS CTR. GEO. MASON U. 23 (Nov. 11, 2015), https://www.mercatus.org/research/research-papers/cutting-red-tape-canada-regulatory-reform-model-united-states [https://perma.cc/64MK-GSE9].

[169] *See* Leora Klapper, Luc Laeven & Raghuram Rajan, *Entry Regulation as a Barrier to Entrepreneurship*, 82 J. FIN. ECON. 591, 622 (2006).

[170] *See, e.g.*, JOSEPH J. CORDES, SUSAN E. DUDLEY & LAYVON Q. WASHINGTON, REGULATORY COMPLIANCE BURDENS: LITERATURE REVIEW & SYNTHESIS 1 (2022), https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2022-10/regulatory_compliance_burdens_litreview_synthesis_finalweb.pdf [https://perma.cc/8B7S-AU3D] ("Government regulation . . . can impose unnecessary administrative burdens as well as barriers to entry into the market of smaller and newer, more innovative, firms."); CHRISTIAN SANDSTRÖM, KARL WENNBERG & NILS KARLSON, BUREAUCRATS OR MARKETS IN INNOVATION POLICY? 84-87 (2019), cms.ratio.se/app/uploads/2019/11/bureaucrats-or-markets-in-innovation.pdf [https://perma.cc/UXE6-TDJK] ("The level of entry barriers to firms entering an industry play an important role in determining prices. Regulations create higher entry barriers and, thus, limited renewal of the economy and reduced competitiveness.").

[171] MARC LABONTE, CONG. RSCH. SERV., R43999, AN ANALYSIS OF THE REGULATORY BURDEN ON SMALL BANKS 28 (2015).

environmental regulations inhibit entry by new firms into a variety of manufacturing industries.[172]

There is little dispute that the GDPR specifically imposes non-trivial compliance costs, even on the largest companies. Meta's average revenue per user in the European Union is less than a quarter of its average revenue per user in the United States and Canada,[173] and industry analysts regularly suggest that European privacy law is responsible for the company's diminished ability to monetize Europeans' attention.[174] The fact that Meta allegedly makes more money in the United Kingdom — where the GDPR does not apply — than it does in the rest of Europe combined supports their theory.[175]

The GDPR's regulatory burden initially led a significant number of domestic news websites to simply block traffic from the European Union rather than comply with the law.[176] Months after the law's effective date, more than a third of the hundred largest U.S. newspapers remained unavailable in the European Union,[177] though the largest

---

[172] *See* Thomas J. Dean & Robert L. Brown, *Pollution Regulation as a Barrier to New Firm Entry: Initial Evidence and Implications for Future Research*, 38 ACAD. MGMT. J. 288, 299 (1995).

[173] Ben Thompson, *Meta's Low E.U. ARPU, The Supreme Court and Section 230*, STRATECHERY (May 23, 2023), stratechery.com/2023/metas-low-e-u-arpu-the-supreme-court-and-section-230/ [https://perma.cc/N8A5-EKCT] [hereinafter Thompson, *Meta's Low E.U. ARPU*].

[174] *See* Ben Thompson, *An Interview with Eric Seufert About Meta's Earnings and the Google–DOJ Case*, STRATECHERY (Feb. 2, 2023), stratechery.com/2023/an-interview-with-eric-seufert-about-metas-earnings-and-the-google-doj-case/ (suggesting that European data-protection rulings will result in a "carve out of Europe" with "decreased monetization there"); Ben Thompson, *An Interview with Eric Seufert About Streaming Advertising, Generative AI, and Marketing Automation*, STRATECHERY (May 25, 2023), stratechery.com/2023/an-interview-with-eric-seufert-about-streaming-advertising-generative-ai-and-marketing-automation/ [hereinafter Thompson, *An Interview about Streaming*].

[175] *See* Thompson, *Meta's Low E.U. ARPU*, *supra* note 173 (quoting Meta's Chief Financial Officer).

[176] *See* Colin Lecher, *Major US News Websites Are Going Down in Europe as GDPR Goes Into Effect*, VERGE (May 25, 2018, 8:23 AM), theverge.com/2018/5/25/17393894/gdpr-news-websites-down-europe [https://perma.cc/2YBN-TMJF].

[177] Jeff South, *More than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect*, NIEMANLAB (Aug. 7, 2018, 12:05 PM),

publishers — like the *New York Times* and the *Washington Post* — never excluded EU readers.[178] What accounts for the discrepancy between small and large publishers' ability to swiftly comply with the new mandate? Large companies have a vast well of resources on which to draw for hiring the lawyers, data scientists, and programmers necessary to comply.

In one of the most thorough investigations into the GDPR's competitive effects, Damien Geradin, Theano Karanikioti, and Dimitrios Katsifis argue there are five reasons that the GDPR has specifically advantaged Google in the advertising technology sector.[179] Among them are Google's vast resources for hiring lawyers, data experts, and programmers.[180] But GDPR compliance goes further, requiring entities to adopt technical and organizational measures and to monitor and document data flows.[181] These measures exhibit "economies of scale and scope," they explain, and thereby "create a competitive advantage for large organizations."[182]

The advantages of scale go further. Ari Waldman has uncovered the realities of how companies are responding to and attempting to comply with new privacy laws, including the GDPR and the CCPA.[183] As he puts it, "[w]ealthier companies also have the resources to build larger in-house privacy departments that can dedicate time, money, and labor to compliance practices. . . . By contrast, smaller companies are forced to outsource more of their compliance to privacy technology vendors."[184]

niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/ [https://perma.cc/G2XN-M97T].

[178] *See* Neil Thurman, James Sly, Bartosz Wilczek & Richard Fletcher, *Forbidden Fruit or Soured Grapes? Long-Term Effects of the Temporary Unavailability and Rationing of US News Websites on Their Consumption from the European Union*, 84 INT'L COMMC'N GAZETTE, 698, 699 (2022).

[179] Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: How a Well-Intended Regulation Ended Up Favouring Large Online Platforms — the Case of Ad Tech*, 17 EUR. COMPETITION J. 47, 63 (2021).

[180] *Id.* at 64.

[181] *Id.*

[182] *Id.*

[183] *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 105-61 (2021).

[184] Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1261 (2022).

He details how vendors purport to offer services that range from assessment and consent-management software to automated incident-response tools and de-identification systems.[185] These software solutions, as Waldman notes, are troubling across several dimensions,[186] but one is surely their asymmetrical implications: large companies have the resources to build in-house compliance regimes that have lower ongoing costs to maintain; smaller companies turn to third-party vendors because they're unable to afford the upfront costs, and as a result, they pay a regular, ongoing premium — each vendor's profit margin — as the cost of foregoing those fixed investment costs.

The widespread conventional wisdom among analysts is thus that the GDPR benefitted the biggest companies to the detriment of smaller ones and that European policymakers are now attempting to course-correct by targeting larger companies with greater precision.[187]

But the GDPR is not just a workaday example of a law that imposes high compliance costs. Rather, the realities of digital markets and the GDPR's consent-based paradigm exacerbate the dynamic. Researchers publishing both before and after the GDPR's implementation have argued that larger firms find it easier to obtain consent because they offer users more easily verifiable benefits in exchange for data collection.[188] This makes intuitive sense: it's difficult for many people to imagine losing access to Google's many services — search, mapping, email, YouTube, and more — whereas newer businesses with incomplete or inchoate products present a more dubious value

[185] *See* Ari Ezra Waldman, Reflection, *Outsourcing Privacy*, 96 NOTRE DAME L. REV. 194, 199-203 (2021).

[186] *See id.* at 203-09.

[187] *See, e.g.*, Kim Mackrael & Sam Schechner, *America's Tech Giants Rush to Comply With New Curbs in Europe*, WALL ST. J. (Aug. 20, 2023, 2:55 PM), https://www.wsj.com/tech/americas-tech-giants-rush-to-comply-with-new-curbs-in-europe-2076ade9 ("The [Digital Markets Act and Digital Services Act] differ [from the GDPR] because they focus on the biggest tech platforms. Analysts say that is in part because the GDPR imposed heavy compliance costs on many small businesses, putting them at a disadvantage compared with their better-resourced competitors.")

[188] *See* James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 48 (2015); Geradin et al., *supra* note 179, at 67.

proposition.[189] After all, about two-thirds of internet users between the ages of fourteen and twenty-nine classify Google Search as "absolutely essential."[190]

Large companies with a wide array of services also only need to obtain consent once, whereas firms with piecemeal offerings must individually and repeatedly seek consent.[191] "Users faced with repetitive requests to consent to the collection and processing of their data are more likely to refuse granting the required consent."[192] And once dominant firms with myriad products and services obtain that single consent, the prevailing interpretation of the GDPR allows unfettered internal sharing. Geradin and his coauthors harshly criticize this aspect of the GDPR: while data protection authorities "have imposed limits on *external* data transfers (data transfers between different companies), they have not done anything to limit any *internal* data sharing within various units of large digital platforms."[193] They argue that this "inadequate enforcement of GDPR's purpose limitation principle not only constitutes a major threat to user privacy, but also places large, dominant platforms, which can combine consent requirements for all their data uses, in a competitive advantage."[194] In other words, entrenched incumbents not only face lower, easier-to-bear compliance costs, they also find it comparatively easier to obtain users' consent and to put that data to use across their platforms.

Perhaps most significant, however, is the cost structure of software development. Unlike many physical or analog businesses, digital businesses have a yawning disparity between their upfront costs and marginal costs. Designing and coding a software product is initially extremely expensive, but the cost difference between delivering that software experience to one hundred or one-hundred million users is

189 *See* Geradin et al., *supra* note 179, at 67.

190 *Id.*

191 *Id.*

192 *Id.*

193 *Id.* at 74.

194 *Id.*

relatively trivial.[195] Consent mechanisms are simply software features, meaning that companies both big and small must design similar software experiences to comply with privacy rules like the GDPR. The result is that Meta can amortize those upfront costs across Facebook's nearly three billion active monthly users, whereas BeReal has similar costs to defray across a user base that's just one percent as big.[196]

Together, these dynamics constitute the power to comply. Large firms have comparatively little difficulty obtaining users' consent to collect and process information because they have enormous resources for hiring lawyers and programmers. Those services exhibit economies of scale, and the burgeoning privacy-compliance industry means that smaller companies will outsource many compliance tasks and pay a premium for the privilege. At the same time, the consent-and-control approach ensures that incumbents will have comparatively little trouble making the case to consumers that their data-for-access value proposition is worth it, and they're able to amortize the fixed, up-front costs of consent and rights-assertion software experiences across a far larger number of users.

B. The Power to Restrict

Incumbency's second advantage is the power to restrict.

There is a fundamental tension between competition and the user-control paradigm at the heart of modern privacy law: increased data access and limited restrictions on information flows will tend to benefit competition but undermine user control, and vice versa. Mandates that increase data accessibility therefore provide insurgent firms with an avenue for challenging a dominant incumbent. By the same token, though, those mandates threaten the principles underlying modern privacy laws. The converse is also true: policies that restrict data access in the name of protecting privacy deprive insurgents of an instrument for challenging established firms, and they thereby benefit the largest

[195] *See* Ben Thompson, *What Is a Tech Company?*, STRATECHERY (Sept. 3, 2019), stratechery.com/2019/what-is-a-tech-company/ [https://perma.cc/63AD-Y4BH] [hereinafter, Thompson, *What is a Tech Company?*].

[196] For a discussion of Facebook's active monthly users, see Thompson, *supra* note 173; for BeReal's, see David Curry, *BeReal Revenue and Usage Statistics*, BUS. OF APPS (Apr. 18, 2024), businessofapps.com/data/bereal-statistics/ [https://perma.cc/4RK9-FRT2].

companies. But incumbency's power to restrict goes beyond this core tension. Data does not fall neatly within existing legal regimes of property rights, intellectual or otherwise. This makes it at least somewhat challenging for large companies to assert legal rights over the information they collect from their users. Consent-based privacy laws supply the next-best alternative, though: unable to undercut rivals by asserting copyright, patent, or trademark rights over their databases, large companies instead cite their users' privacy rights. After all, the terms of service authorize information collection and processing by the largest platforms — but *only* by them — and we just saw how the largest platforms have the least trouble obtaining consent. So, privacy law becomes another competitive tool for the largest companies, providing them with novel legal authority for restricting putative rivals' access to their financially lucrative and otherwise difficult-to-control input.

Examples abound of how access to data can provide a competitive edge. *hiQ Labs v. LinkedIn* is a prominent example already discussed: hiQ's software product was built on the back of LinkedIn users' data, and LinkedIn specifically cited privacy concerns to justify blocking hiQ's access at the same time that LinkedIn was launching a competing software product.[197] Social networking sites have repeatedly illustrated the dynamic. In 2010, Twitter launched a tool that allowed its users to find their Facebook friends on Twitter.[198] The same day the feature launched, Facebook blocked it.[199] Three years later, Mark Zuckerberg personally approved the same-day blocking of the Twitter-owned short-form video app Vine's friend-finding feature.[200] Instagram famously

[197] *See supra* notes 144–150 and accompanying text.

[198] MG Siegler, *Twitter Perfects a Way To Link Up With Your Facebook And LinkedIn Friends*, TECH CRUNCH (June 23, 2010, 3:00 PM), techcrunch.com/2010/06/23/twitter-facebook-friends-linkedin/ [https://perma.cc/8B7N-S34V].

[199] MG Siegler, *Wow That Was Fast — Facebook Blocks Twitter's Way to Look Up Friends*, TECH CRUNCH (June 23, 2010, 3:12 PM), techcrunch.com/2010/06/23/facebook-blocks-twitter/ [https://perma.cc/7LK9-HRY2].

[200] Adi Robertson, *Mark Zuckerberg Personally Approved Cutting Off Vine's Friend-Finding Feature*, VERGE (Dec. 5, 2018, 7:35 AM), theverge.com/2018/12/5/18127202/mark-zuckerberg-facebook-vine-friends-api-block-parliament-documents [https://perma.cc/G3V5-QPMB] (citing UK Parliament Report, Ex. 44, at *15, *available at* parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf).

bootstrapped its social network via access to Twitter's API, which Twitter eventually also blocked.[201] In each instance, a competition mandate that required social networks to allow users to export and replicate their social or interest graphs across multiple services would raise privacy concerns — after all, if we are mutual friends on Facebook and you export your social graph to Twitter, you are sharing data about me with Twitter without my consent to do so.

There are indications that access to vast amounts of data is an increasingly valuable competitive resource. After it came to light that OpenAI used Reddit's APIs to train its large language models, Reddit restricted API access and imposed steep costs explicitly for the purpose of extracting payment from other artificial-intelligence developers — a ploy that led Google to pay $60 million annually to license Reddit's data for large-language-model training.[202] Reddit's cofounder and chief executive explained, "The Reddit corpus of data is really valuable. . . . But we don't need to give all of that value to some of the largest companies in the world for free."[203] Users posting on Reddit did not consent to have their posts ingested into the models that power ChatGPT and its competitors, though competition-minded folks are excited at the prospect of AI chatbots disrupting Google's dominance in search.[204]

---

[201] *See* Ben Thompson, *The Web's Missing Interoperability*, STRATECHERY (Mar. 2, 2021), stratechery.com/2021/the-webs-missing-interoperability/ [https://perma.cc/3P7T-X39Y] [hereinafter Thompson, *The Web's Missing Inoperability*]; Alexia Tsotsis, *No API For You: Twitter Shuts Off "Find Friends" Feature For Instagram*, TECH CRUNCH (July 26, 2012, 12:44 PM), techcrunch.com/2012/07/26/no-api-for-you-twitter-shuts-off-find-friends-feature-for-instagram/ [https://perma.cc/YQ9R-UV82].

[202] Anna Tong, Echo Wang & Martin Coulter, *Exclusive: Reddit in AI Content Licensing Deal With Google*, REUTERS (Feb. 21, 2024, 8:10 PM), https://www.reuters.com/technology/reddit-ai-content-licensing-deal-with-google-sources-say-2024-02-22/.

[203] Mike Isaac, *Reddit Wants to Get Paid for Helping to Teach Big A.I. Systems*, N.Y. TIMES (Apr. 18, 2023), nytimes.com/2023/04/18/technology/reddit-ai-openai-google.html.

[204] *Cf.* Nico Grant & Cade Metz, *A New Chat Bot Is a 'Code Red' for Google's Search Business*, N.Y. TIMES (Dec. 21, 2022), nytimes.com/2022/12/21/technology/ai-chatgpt-google-search.html (detailing Google's internal struggles to respond to ChatGPT); Akash Sriram & Chavi Mehta, *OpenAI Tech Gives Microsoft's Bing a Boost in Search Battle With Google*, REUTERS (Mar. 22, 2023, 11:34 AM), reuters.com/technology/openai-tech-gives-microsofts-bing-boost-search-battle-with-google-2023-03-22/ (suggesting that OpenAI's integration into Bing was — at least temporarily — helping siphon traffic from

Antitrust scholars have in their own way begun recognizing the tension. Erika Douglas, for example, argues at length that undercutting competition to further privacy objectives is inconsistent with vast swaths of antitrust doctrine.[205] Douglas has been skeptical of LinkedIn's attempts to justify its conduct towards hiQ, and she has been critical of Apple's privacy-and-security-related justifications for excluding Epic from the App Store.[206] Noting that data is nonrivalrous — it can be copied for essentially no cost and using it does not deplete it — Maurice Stucke observes that the efficiency-maximizing, optimal economic arrangement is for data to be shared widely.[207] Implementing competition policies that maximize data distribution, however, clashes with the aims of privacy law.[208]

One consequence of the tension is that antitrust remedies will exacerbate privacy concerns. In evaluating antitrust law's promise for constraining surveillance-based businesses, Julie Cohen notes that "antitrust interventions designed to extend data flows outside the licensing ecosystems of dominant entities will only make privacy problems worse if they are not paired with other, privacy-focused interventions."[209] Industry and their allies have howled with indignation that Europe's new competition laws threaten privacy and security by

Google); Ben Thompson, *AI and the Big Five*, STRATECHERY (Jan. 9, 2023), stratechery.com/2023/ai-and-the-big-five/ [https://perma.cc/3H34-WR34] [hereinafter Thompson, *AI and the Big Five*] (theorizing about the impacts of generative AI on the largest tech companies).

[205] *See, e.g.*, Douglas, *Justification*, *supra* note 142, at 457-65 ("Privacy restraints are not justified when the defendant's claim is that privacy benefits consumers, and such privacy is only reasonably achievable by limiting competition. . . . Supreme Court precedent is clear that such arguments do not constitute a procompetitive justification.").

[206] *See id.* at 466-70 (noting with approval that the district and circuit courts in *hiQ* were skeptical of LinkedIn's privacy justifications); *id.* at 462 ("[T]he [district] court in *Epic v. Apple* erred in accepting Apple's first 'security' justification, which was premised on an improvement of privacy quality unrelated to competition . . . . [Apple's] purported justification amounts to an assertion that the privacy restraints are 'good' for consumers, regardless of their effects on competition. This is not a cognizable justification in antitrust law.").

[207] *See* Stucke, *supra* note 116, at 411-13.

[208] *See id.*

[209] Cohen, *supra* note 48, at 10 (emphasis omitted).

opening up closed and integrated products and services.[210] Matthew Sipe illustrates the dynamic by pointing to an ongoing dispute between Tile and Apple.[211] Both companies make Bluetooth-tracking devices, but Apple confers data privileges on its own trackers that are unavailable to Tile's. "Tile thus seeks weaker default privacy settings . . . in the name of competition."[212]

The web advertising business provides another apt example. It is highly concentrated, with Google controlling as much as ninety percent of some aspects of the programmatic advertising infrastructure.[213] The Department of Justice and a host of state attorneys general are suing Google for engaging in allegedly anticompetitive conduct in its web advertising business, and the plaintiffs are seeking — among other relief — breakups of the Google advertising business.[214] Imagine for a moment the suits are successful and Google's web advertising infrastructure is broken up and spun out into potentially dozens of individuals firms. Due to the integrated nature of programmatic advertising and its reliance on licensed data flows, users browsing the web would go from having a single company conducting the vast majority of privacy-invasive

[210] *See, e.g.*, John Gruber, *Apple Adjusts DMA Plan to Offer Direct Downloading of Apps From the Web (With a Big Asterisk), Custom Link-Out Screens, and Marketplaces Solely for the Distribution of a Developer's Own Apps*, DARING FIREBALL (Mar. 13, 2024), daringfireball.net/2024/03/apple_adjusts_dma_plan [https://perma.cc/NZ6A-5SYK] ("[T]he DMA wants to have its cake and eat it too. It requires Apple both to open up iOS to additional methods of software distribution *and* to keep iOS as secure as possible."); John Gruber, *Apple Disables WebKit's JIT in Lockdown Mode, Offering a Hint Why BrowserEngineKit Is Complex and Restricted*, DARING FIREBALL (June 24, 2024), https://daringfireball.net/2024/06/apple_disables_webkits_jit_in_lockdown_mode [https://perma.cc/L6G2-P4GC] (describing how a DMA mandate concerning browser engines can threaten device security); John Gruber, *Apple's Plans for the DMA in the European Union*, DARING FIREBALL (Jan. 26, 2024), daringfireball.net/2024/01/apples_plans_for_the_dma [https://perma.cc/2EFZ-NU5E] (quoting Press Release, *Apple Announces Changes to iOS, Safari, and the App Store in the European Union*, APPLE (Jan. 25, 2024), apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/ [https://perma.cc/5ELY-CDBD]).

[211] *See* Sipe, *supra* note 18, at 396-97.

[212] *Id.* at 396.

[213] *See* Geradin et al., *supra* note 179, at 64 n.64.

[214] *See* Miles Kruppa & Dave Michaels, *DOJ Sues Google, Seeking to Break Up Online Advertising Business*, WALL STREET J. (Jan. 24, 2023, 4:59 PM), wsj.com/articles/u-s-sues-google-for-alleged-antitrust-violations-in-its-ad-tech-business-11674582792.

processing in house, to dozens of firms sharing personal information to deliver a similar experience. Competition may be improved, but it would come at the expense of further undermining users' ability to know and control who processes their information.[215]

[215] Of course, one could object that the distribution of information inside one dominant firm is no better or worse from a privacy perspective than information flowing across multiple smaller firms. Wide distribution of personal data may raise increased information *security* concerns, the objection goes, but security and privacy aren't interchangeable. *Cf.* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013) ("Legal scholarship tends to conflate privacy and security. However, security and privacy can, and should, be treated as distinct concerns."); Daniel J. Solove & Woodrow Hartzog, *Unifying Privacy and Data Security*, *in* BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022) ("Right now, there is a schism between privacy and security in companies. Privacy functions are commonly addressed by the compliance and legal departments, while security is handled by the information technology department. The two areas are commonly split apart and rarely speak to each other."). It's true that under the traditional paradigm that conflates privacy and secrecy, privacy is seemingly not degraded when previously disclosed information is shared more widely. *Cf.* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 21-24 (2008) (explaining privacy as secrecy). But not only have scholars thoroughly debunked the privacy-as-secrecy paradigm, *see, e.g.*, *id.* ("Although these violations are clearly not the same, courts and policymakers frequently have a singular view of privacy in mind when they assess whether an activity violates privacy. As a result, they either conflate distinct privacy problems despite significant differences or fail to recognize a problem entirely. In short, privacy problems are frequently misconstrued or inconsistently recognized in the law."), every richer theoretical account of privacy also considers the flow of information from one to many actors a core privacy problem — including privacy as confidentiality, obscurity, trust, and contextual integrity. *See* Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 134 (2007); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1344-45 (2015); ARI EZRA WALDMAN, PRIVACY AS TRUST 93-107 (2018); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129-57 (2010). And the wide proliferation of user data that would result from breaking up Google's advertising-infrastructure monopoly would also undermine the user-control paradigm underlying recent state privacy laws. *See supra* note 44 (accepting the user-control paradigm as the operative definition of privacy for purposes of this Article). For a memorable illustration of the byzantine structure of the ad tech industry 15 years ago, *see* John Ebbert, *New Ad Tech Ecosystem Map Released by LUMA Partners' Kawaja*, ADEXCHANGER (September 27, 2010, 12:04 AM) https://www.adexchanger.com/venture-capital/ecosystem-map-luma-partners-kawaja/ [https://perma.cc/5MNK-7ABU]; *see also* Seb Joseph, *'Nothing Makes Sense Anymore': What's Driving Ad Tech's Latest Consolidation Wave*, DIGIDAY (Feb. 23, 2021), https://digiday.com/marketing/ad-techs-latest-consolidation-wave/ [https://perma.cc/98ZH-4YNV] (describing consolidation in

Competition mandates can thus threaten privacy law's user-control paradigm. But the arrow points in the other direction too — privacy rules constrain data flows, and constraints on data flows benefit incumbents at the expense of insurgents.

Geradin and his coauthors note that companies have become quite reluctant to share data for fear of running afoul of the GDPR. Sharing has become "risky and many data holders may decide to take the extreme measure of refusing to share their data with smaller ad tech players as they may not trust their ability to comply with the GDPR."[216] This ultimately benefits incumbents because "these smaller actors are generally the ones that would benefit the most from accessing third-party data," since "large market actors holding massive amounts of data . . . already capture the data they need within their ecosystem."[217] And they specifically show how Google has wielded the GDPR as a cudgel for further entrenching itself against upstart advertising technology firms. For example, on the eve of the GDPR's effective date, Google restricted access to the DoubleClick ID — a unique, cookie-based identifier assigned by Google to individuals, which allowed advertisers to independently track conversions and attribution — and Google cited the GDPR for the policy change.[218] After the policy change, advertisers have no option but to trust Google to evaluate the effectiveness of Google's own advertising, a move that industry analysts have called "'leveraging privacy concerns as a pretext' to further raise the walls of Google's garden."[219]

the ad tech sector in recent years). On the other hand, it may well be that dominant firms' internal data flows today violate informational norms, a question that receives nuanced treatment in Kirsten Martin, *Platforms, Privacy, and the Honeypot Problem*, 37 HARV. J. L. & TECH. 1087, 1109-15 (2023). The further distribution of data that would result from breaking up such firms would, nevertheless, create its own distinct violations of informational norms.

[216] Geradin et al., *supra* note 179, at 67-68.

[217] *Id*.

[218] *See id.* at 81-83 (citing Alison Weissbrot, *Google Sharply Limits DoubleClick ID Use, Citing GDPR*, AD EXCHANGER (Apr. 27, 2018, 1:51 PM), adexchanger.com/platforms/google-sharply-limits-doubleclick-id-use-citing-gdpr/ [https://perma.cc/Y6S9-WRFL]).

[219] *Id.* at 83 (citing Robin Jurzer, *Google to Stop Media Buyers from Using DoubleClick IDs, Keeping Measurement & Attribution within Its "Walled Garden"*, MARTECH TODAY (May 14, 2018, 10:52 AM), martechtoday.com/google-to-stop-media-buyers-from-using-doubleclick-ids-keeping-measurement-attribution-within-its-walled-garden-215246

Relevant here too is their argument about the competitive effects of the prevailing interpretation of the GDPR's purpose limitation.[220] Larger companies with multiple products face no restrictions on the internal sharing of data: Google uses your Maps queries and Gmail metadata to target advertising on web search, and Meta uses the contacts you uploaded to WhatsApp to suggest friends and follows on Facebook and Instagram. Upstarts with limited or singular offerings don't have an enormous well of data collected elsewhere to effectively subsidize their products.

Other researchers have empirically documented how the GDPR has led to increased concentration in web technology services, and "although all firms suffer losses, the largest vendor — Google — loses relatively less and significantly increases market share in important markets such as advertising and analytics."[221]

Privacy laws, to be fair, don't exclusively constrain data flows. The GDPR and the CCPA, for example, include data portability rights, which empower individuals to receive their personal data in a format that allows them to switch service providers.[222] Portability rights have dueling justifications: they provide individuals with greater control over their information — a classic touchstone of both the European data-protection regime and the American consent-and-control approach to information privacy — and they also have beneficial effects on competition.[223] At the same time, portability rights pit users' control rights in a zero-sum contest: "[T]here is a tension between opening data flows, to promote competition and innovation, provide user control,

[https://perma.cc/5SUP-GZYP]; George Slefo, *Google's Removal of DoubleClick ID Presents Litany of Issues for Brands, Agencies*, ADAGE (May 8, 2018), adage.com/article/digital/google-s-move-remove-doubleclick-id-presents-issues/313415).

[220] *See supra* notes 193–194 and accompanying text.

[221] Christian Peukert, Stefan Bechtold, Michail Batikas & Tobias Kretschmer, Regulatory Spillovers and Data Governance: Evidence from the GDPR, 41 MARKETING SCIENCE 746, 746 (2022).

[222] *See* Chander et al., *supra* note 14, at 1752-53.

[223] *See id.* (citing Art. 29 Data Prot. Working Party Guidelines on the Right to Data Portability, at 3-4 (2017)).

and for other reasons, and closing data flows, for reasons including protecting privacy and cybersecurity."[224]

All of this goes to show that there is an aspect of constraining data access that indelibly advantages incumbents. But consent-and-control privacy rules are more pernicious yet. Scholars have observed how the business practices of the information economy don't fit neatly within existing legal doctrines.[225] Amy Kapczynski explains: "[T]he most critical technological inputs and outputs of the data-driven algorithmic age are unowned, if ownership means exclusive rights that carry a 'good-against-the-world' quality."[226] Algorithms are categorically excluded from patent law, "and machine-learning techniques are arguably discovering patterns in nature that cannot be propertized. Nor are these techniques readily protectable via copyright."[227] And the underlying data itself is "famously unowned in intellectual-property terms."[228]

In the absence of a legal regime of strong and well-demarcated ownership interests to assert, platforms must turn to other, more subtle forms of control. Julie Cohen, for example, argues that companies use trade-secrecy and contract law to "mark data flows with indicia of ownership."[229] While "intellectual property theory places 'facts' permanently in the public domain," Cohen argues, "intellectual property practice traditionally has recognized a need for gap-filling protection in certain industries, and has looked to trade secrecy and contract law to fulfill that need."[230] Cohen focuses specifically on how

---

[224] Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Security, and Other Considerations*, 6 GEO. L. TECH. REV. 57, 57-58 (2022); *see also* Wenlong Li, *A Tale of Two Rights: Exploring the Potential Conflict Between Right to Data Portability and Right to be Forgotten Under the General Data Protection Regulation*, 8 INT'L DATA PRIV. L. 309 (2018), doi.org/10.1093/idpl/ipy007 [https://perma.cc/P2RB-WSUQ].

[225] *See, e.g.*, Amanda Parsons & Salomé Viljoen, *Valuing Social Data*, 124 COL. L. REV. 993, 993 ("[S]ocial data production also presents critical challenges for the legal regimes that encounter it.").

[226] Amy Kapczynski, *The Law of Information Capitalism*, 129 YALE L.J. 1460, 1500 (2020).

[227] *Id.* at 1501.

[228] *Id.*

[229] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 62 (2019).

[230] *See id.* at 63.

platform companies use contracts with those who require access to the platforms' data and algorithms to insist on secrecy, confidentiality, and non-disclosure.[231]

But contract law — and privacy law's reliance on user-control rights — has further-reaching consequences for large platforms. Beyond simply binding their counterparties to secrecy, privacy law's consent paradigm offers the large platforms a novel legal basis for restricting others' access to their data. Contract law empowers companies to manipulate the terms of consent, and scholars have exhaustively documented that no one reads them.[232] Working in tandem with their ease in obtaining consent,[233] these phenomena empower companies to effortlessly obtain consent to data collection and processing but on the company's own terms — terms that are highly unfavorable to the incumbents' competitors. Consent-based rules therefore give incumbents a potent one-two punch: users have consented to collection and processing by us *but only by us*.

It is for this exact reason that LinkedIn can argue it is bound by its own terms of service and by the FTC's consumer-protection mandate to prevent hiQ from scraping and using LinkedIn's users' data.[234] Now,

[231] *Id.* at 45.

[232] On the former, see *supra* notes 81–88 and accompanying text; on the latter, see, for example, Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 143 (2013) ("Privacy policies are notoriously ineffective at providing information to consumers about online businesses' data practices."); Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMMC'N & SOC'Y 128, 140-42 (2020) ("The results of this study suggest that individuals often ignore privacy and TOS policies for social networking services."); Michael Karanicolas, *Too Long; Didn't Read: Finding Meaning in Platforms' Terms of Service Agreements*, 52 U. TOL. L. REV. 1, 3, nn.6–8 (2021) ("It has become a common trope to note the near-universal ignorance of consumers regarding the conditions that they acquiesce."); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y. 543, 543 ("In this paper we content that the time to read privacy policies is, in and of itself, a form of payment.").

[233] *See supra* notes 81–82 and accompanying text.

[234] Douglas argues that the district and circuit courts' skepticism of LinkedIn's privacy arguments is inconsistent with the FTC's privacy jurisprudence, *see* Douglas, *supra* note 142, at 468-69 ("Th[e courts'] skepticism is at odds with the FTC's fundamental assumption in Section 5 FTC Act enforcement that reasonable expectations of privacy are established by the terms of privacy policies. The FTC

LinkedIn only advanced a strong version of that argument in its unsuccessful cert. petition at the Supreme Court, though it's telling to understand why.[235] The parties' dispute was fully briefed at the Ninth Circuit in 2017 — a year before the GDPR went into effect and the CCPA was enacted.[236] At that time, LinkedIn was one of the few major tech platforms that wasn't under a consent decree with the FTC related to its privacy practices.[237] So in a world where the GDPR, CCPA, and other state laws impose a host of additional legal obligations on user data, LinkedIn's privacy arguments become considerably stronger. In 2017, LinkedIn only argued that protecting user privacy tipped the equitable scales in its favor, but today LinkedIn can assert a legal duty to cut off

premises its privacy enforcement on the longstanding view that companies which make express or implied promises 'simply ha[ve] to keep them.'"), but as far as I know, LinkedIn did not argue at the district or circuit court that the threat of FTC enforcement legally compelled them to block hiQ's access.

[235] *See supra* notes 145–146; Petition for a Writ of Certiorari, LinkedIn Corp. v. hiQ Labs, Inc., 141 S. Ct. 2752, *petition for cert. filed* (Mar. 9, 2020) (No. 19-1116).

[236] *Id.*

[237] LinkedIn is one of the only social networks that has never been the subject of FTC enforcement, though Microsoft — its parent company — has been. *See Cases Tagged with Privacy and Security*, FTC, ftc.gov/enforcement/cases-proceedings/terms/1420 (last visited July 28, 2023) [https://perma.cc/GKR7-4AR4]. Microsoft settled with the FTC in 2002 over allegations that the company misrepresented its privacy and security practices to users of its Passport web services. *See* Agreement Containing Consent Order, *In the Matter of Microsoft Corp.*, FTC, No. C–4069 (Dec. 20, 2002). That consent decree expired in December 2022. *See* Decision & Order, *In the Matter of Microsoft Corp.*, FTC, No. C–4069, at 4 (Dec. 20, 2002). Microsoft agreed to settle again with the FTC in June 2023 over allegations that the company's Xbox Live gaming service violated the Children's Online Privacy Protection Act. *See* Press Release, *FTC Will Require Microsoft to Pay $20 Million Over Charges it Illegally Collected Personal Information from Children Without Their Parents' Consent*, FTC (June 5, 2023), ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information [https://perma.cc/MBX3-AJN4]. It's not clear that either the Passport or Xbox Live consent decrees apply to LinkedIn, and in any event, the FTC never sought to punish LinkedIn for failing to stop hiQ. LinkedIn is currently under investigation by the Irish Data Protection Commission for violating the GDPR with its ad-targeting practices, but those allegations do not involve hiQ's scraping either. *See* Yuvraj Malik, *Microsoft Flags Over $400 Mln Charge for Irish Privacy Violation Fine on LinkedIn*, REUTERS (June 1, 2023, 10:29 AM), reuters.com/technology/microsoft-flags-over-400-mln-charge-irish-privacy-violation-fine-linkedin-2023-06-01/ [https://perma.cc/E4FP-VGZR].

hiQ's access because LinkedIn faces the threat of privacy-law enforcement actions if it fails to honor its own terms of service. Where companies previously lacked property-like rights over the data they collect on their users, privacy law supplies the next-best alternative. Under either regime, the platforms have a legal basis for restricting others' access to their engine of value production.

For another illustration of privacy as a next-best alternative to property, consider the scuffle between Meta and the NYU Ad Observatory. The latter is an academic research group created to examine the origin and spread of political advertising on Facebook.[238] They explain that their aim is to reveal who pays for political ads on the platform and understand how those ads are targeted.[239] The researchers collected data through a browser plugin that automatically collects data about the political ads that appear in the user's feed; according to the researchers, the plugin doesn't collect any personally identifying information.[240] After their work produced several embarrassing stories about Facebook's practices,[241] Meta banned the researchers' accounts and justified its moves with a blog post headlined, "Research Cannot Be

[238] *See* James Vincent, *Facebook Bans Academics Who Researched Ad Transparency and Misinformation on Facebook*, THE VERGE (Aug. 4, 2021, 4:08 AM), theverge.com/2021/8/4/22609020/facebook-bans-academic-researchers-ad-transparency-misinformation-nyu-ad-observatory-plug-in [https://perma.cc/N75H-C88N] (citing Nancy Watzman, *The Political Ads Facebook Won't Show You*, CYBERSECURITY FOR DEMOCRACY (May 12, 2021), medium.com/cybersecurity-for-democracy/the-political-ads-facebook-wont-show-you-e0d6181bca25 [https://perma.cc/7KEL-ZPFJ]).

[239] *Id.*

[240] *Id.*

[241] *See, e.g.*, James Vincent, *Far-Right News and Misinformation Received the Most Engagement on Facebook During 2020 US Election*, THE VERGE (Mar. 4, 2021), theverge.com/2021/3/4/22313013/far-right-news-misinformation-facebook-us-2020-election-nyu-study-engagement [https://perma.cc/5L9G-8LKV] ("[The] takeaway is that, one way or another, far-right misinformation sources are able to engage on Facebook with their audiences much, much more than any other category."); Craig Silverman & Ryan Mac, *Facebook Promised To Label Political Ads, But Ads For Biden, The Daily Wire, And Interest Groups Are Slipping Through*, BUZZFEED NEWS (Oct. 22, 2020, 1:47 PM), buzzfeednews.com/article/craigsilverman/facebook-biden-election-ads [https://perma.cc/5XDT-VWSD] ("With less than two weeks before the US presidential election, Facebook is failing to label who paid for some election ads, including some on behalf of Democratic nominee Joe Biden's campaign.").

the Justification for Compromising People's Privacy."[242] As that title suggests, the company argued that its terms of service prohibit the scraping of data and that the researchers were therefore violating its users privacy by using the browser plugin.[243] This was, of course, not the first time that the company has cut off or restricted rivals' access to its data,[244] and the company would surely trot out the same argument again in the face of new transparency rules.

Privacy mandates also provide entrenched incumbents with a potent weapon that's already surfaced repeatedly: pretext. Rory Van Loo has documented the various moves that companies make to use privacy to pretextually further their business interests — be it to avoid accountability or to undercut putative rivals.[245] As he shows, firms are frequently undercutting competition, transparency, and oversight by exercising ever-greater control over their data, and they're justifying these moves by pointing to privacy law's consent regime.[246] Examples we've seen so far include LinkedIn's attempts to launch a competitor to hiQ, Google's restriction on the DoubleClick ID, and Facebook's ban on the Ad Observatory researchers. Epic Games vociferously argued that Apple's justifications for excluding its game from the App Store — which Apple justified on privacy and security grounds — were pretextual.[247] And Apple's ATT initiative is likely motivated in part by a recognition of its unique position — by virtue of controlling the App Store — to extract greater rent by launching its own app-installation ad network.[248] After

[242] Mike Clark, *Research Cannot Be the Justification for Compromising People's Privacy*, META (Aug. 3, 2021), about.fb.com/news/2021/08/research-cannot-be-the-justification-for-compromising-peoples-privacy [https://perma.cc/WGS3-AV2R].

[243] *See id.*

[244] *See, e.g.*, *FTC v. Facebook, Inc.*, No. 20-cv-03590, Complaint ¶ 23 (D.D.C. Jan. 13, 2021) ("Facebook has made key APIs available to third-party apps *only* on the condition that they refrain from providing the same core functions that Facebook offers . . . and from connecting with or promoting other social networks.").

[245] *See* Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 101, 122-39 (2022).

[246] *See id.*

[247] *See* Findings of Fact and Conclusions of Law Proposed by Epic Games, Inc. at 152-90, Epic Games, Inc. v. Apple, Inc., No. 4:20-cv-05640-YGR-TSH (N.D. Cal. Apr. 8, 2021).

[248] *See, e.g.*, Ben Thompson, *Data and Definitions*, STRATECHERY (June 21, 2022), stratechery.com/2022/data-and-definitions/ [https://perma.cc/RYP2-9ZAL] (arguing that ATT uses a privacy justification to undercut competition).

all, the company gets to bolster its privacy bonafides while at the same time conveniently siphoning off billions of dollars in advertising revenue from Meta, YouTube, and other app-installation advertising destinations.[249]

In sum, when it comes to data-intensive businesses, there is a core tension between competition and the modern approach to privacy law. Insurgents benefit from access to rivals' data, and incumbents are wise to jealousy guard it. Competition mandates and antitrust remedies — acting alone — are thus likely to undermine privacy law. And the opposite is also true, as companies' reaction to the GDPR shows. But the power to restrict goes even further — affording companies a legal basis for exercising property-like control over their data.

C. The Power to Circumvent

A third advantage of incumbency is the power to circumvent. The circumvention power is derived from those discussed previously. Part III.A outlined how the largest companies have access to the most data because they have an unparalleled ability to extract consent from users, and Part III.B detailed how the largest companies have a unique ability to restrict others' access to the data they generate, collect, and process. At sufficient scale, exclusive access to enormous reserves of data confers a distinct advantage — one that allows the biggest companies to render privacy rules largely ineffectual. Privacy rules by their nature deprive everyone of access to some data, but that deprivation becomes increasingly immaterial to informational platforms that have enough data. Since data's value lies in its prediction value, the largest companies can inferentially fill the gaps left by those who withhold their consent. But this circumvention power is available only to the largest companies,

[249] *Cf.* Jay Peters, *Apple Flexes Its Control Over the App Store*, THE VERGE (Oct. 27, 2022, 1:45 PM), theverge.com/2022/10/27/23426993/apple-app-store-rules-guidelines-ads-changes-flexes-control [https://perma.cc/6LDV-F5VG] ("In its changes this week, Apple updated its App Store rules to give itself a cut of some advertising revenue in social media apps and purchase revenue from Web3 apps."); *see also* Ethan Cramer-Flood, *Money is Still Pouring into App Install Ad Spending, Boosting Apple and Others*, EMARKETER (Feb. 16, 2023), emarketer.com/content/money-still-pouring-app-install-ad-spending-boosting-apple-others [https://perma.cc/6TAM-D7YY] (listing Apple's app install ad revenues in 2023 at $5.20 billion — a 26.3% annual increase — and in 2024 at $6 billion).

and as a result, even the most stringent consent-and-control privacy rules have a disparate effect that disadvantages companies with access to less data.

The power to circumvent is rooted in two aspects of data discussed in Part I.B. First, data's economic value is best understood as a function of its prediction value.[250] Amanda Parsons and Salomé Viljoen argue that data "produces value from its capacity to materialize and store traces of human activity," which "allows entities to catalogue, analyze, aggregate and mine such traces for insight, and in turn, to use such insights to predict and modify behavior."[251] Ultimately, they explain, "the value of social data lies in its capacity to predict — and based on such prediction to manage — social behavior."[252] Second, as the collection of data has proliferated and as the cost of computing power has fallen, data scientists have developed and refined increasingly sophisticated techniques for wringing more and more prediction value from any given dataset.[253] No matter what label the techniques parade under — machine learning, artificial intelligence, predictive analytics, big data, or simply statistical regressions — they allow companies to make ever-more precise and profitable inferences about human behaviors subjected to these techniques. Paired with platforms' ability to obtain and shield data, the largest firms with the most data gain the power to infer around privacy laws' restrictions.

Apple's App Tracking Transparency ("ATT") initiative has provided a stark illustration of this circumvention power. By way of reminder, Apple implemented a seemingly minor policy change to several of its software platforms, including iOS, in April 2021: rather than allow consumers to opt out of cross-site and -app tracking, Apple switched the default to an opt-in regime.[254] After ATT took effect, applications that wished to remain in Apple's App Store were required to display a new

[250] *See* Hirsch, *supra* note 75 and accompanying text; *see also* Zuboff, *supra* note 88, at 8, 10, 93-97 (2019).

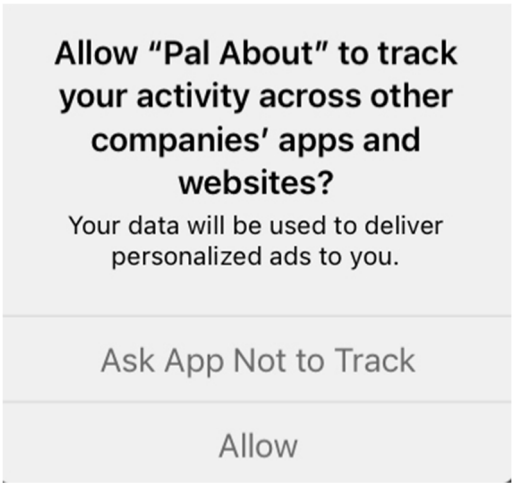
[251] Parsons & Viljoen, *supra* note 225, at 1009-10.

[252] *Id.* at 1010.

[253] *See* Barocas & Nissenbaum, *supra* note 70 and accompanying text.

[254] *See supra* notes 62–64 and accompanying text.

prompt for obtaining users' consent to tracking. An illustrative prompt is displayed below.[255]



While ATT is one company's private initiative, it's nevertheless an illustration of a restrictive consent-based rule with an extremely high rate of compliance.[256] It's not hard to imagine the FTC adopting a similar

[255] For the source of the illustration, see *User Privacy and Data Use*, APPLE, developer.apple.com/app-store/user-privacy-and-data-use/ (last visited July 29, 2024, 12:30 PM) [https://perma.cc/BKN2-DXJD]. App developers can customize the text in the second string — the roman text that reads in the illustration, "Your data will be used to deliver personalized ads to you." Developers also prime users before the prompt is shown, and there is an entire cottage industry that has grown up around designing the ATT-prompt experience to garner the greatest amount of tracking. *See, e.g.*, *How to Increase App Tracking Transparency Opt-in Rates*, ADJUST, adjust.com/glossary/app-tracking-transparency#how-to-increase-app-tracking-transparency-opt-in-rates (last visited Dec. 12, 2023) [https://perma.cc/3GZM-LLHJ] [hereinafter *Increase Transparency*] (providing advice for how to increase ATT opt-in rates).

[256] ATT is restrictive because it's opt-in rather than opt-out like the CCPA. *See, e.g.*, Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1753 (2021) ("Both the CCPA and the GDPR contain a right for individuals to 'opt out' and deny permission for handling of their personal data in certain ways."). It has a high rate of compliance because violations are punishable by removal from the App Store — a devastating consequence for an app developer. *Cf.* Peter Ormerod, *Privacy Qui Tam*, 98 NOTRE DAME L. REV., 279-307 (2022) (discussing low rates of enforcement and compliance with existing privacy laws).

policy through a rulemaking, and the agency may in fact be in the process of doing something similar.[257]

Estimates suggest that most users declined ATT's prompt for cross-site and -app tracking by a wide margin.[258] Critically, this policy change deprived *all* app developers of access to data that is extremely valuable to the online advertising ecosystem. For example, Meta estimated that ATT would cost its business $10 billion in lost revenue in 2022.[259] And for a while after ATT's implementation, Meta's ad sales business did indeed suffer.[260] Yet, two years after ATT was implemented, it became increasingly apparent that Meta has proven adept at absorbing and responding to the ATT-imposed data loss, whereas smaller companies with materially identical business models continue to sputter.[261]

[257] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg.51273 (proposed Aug. 22, 2022) (to be codified at 16 C.F.R. ch. I).

[258] *See* Estelle Laziuk, *iOS 14 Opt-In Rate – Weekly Updates Since Launch*, FLURRY, flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/ (last visited Dec. 12, 2023) [https://perma.cc/U4T3-76KK]. The fact that so many users declined tracking is itself a telling illustration of Part I.B's point about how malleable consent is. ATT is unique in that the vast majority of the prompt is designed by Apple; app developers have extremely limited ability to augment or alter the consent prompt shown to users. *See, e.g.*, *Increase Transparency*, *supra* note 255 (showing how little control developers have over the ATT prompt).

[259] *See* Meghan Bobrowsky, *Facebook Feels $10 Billion Sting from Apple's Privacy Push*, WALL ST. J. (Feb. 3, 2022, 5:22 PM), wsj.com/articles/facebook-feels-10-billion-sting-from-apples-privacy-push-11643898139.

[260] *See, e.g.*, Sarah E. Needleman, *Facebook Posts Slower Sales Growth With Apple Privacy Policy*, WALL ST. J. (Oct. 25, 2021), wsj.com/articles/facebook-expected-to-post-slower-sales-growth-with-apple-privacy-policy-11635154200 ("Facebook's ad sales, its primary revenue source, saw slower growth in the first full quarter since Apple in April started requiring apps to ask users whether they want to be tracked.").

[261] *See, e.g.*, Salvador Rodriguez, *Facebook Parent Meta Platforms Sees First Sales Increase in Nearly a Year*, WALL ST. J. (Apr. 26, 2023), wsj.com/articles/meta-platforms-q1-earnings-report-2023-aa820bcd ("The tough economic climate, an increasing number of regulations limiting personalized ads and the fallout from Apple Inc.'s ad-tracking changes in 2021 have weighed on the digital-ad market . . . . The 3% increase is an improvement from the 4.5% drop in revenue that the company posted in the final quarter of 2022, indicating that Meta's heavy investment in artificial-intelligence tools to improve its ad-targeting systems is working."); Jonathan Vanian, *Snap Plunges on First-quarter Revenue Miss*, CNBC (Apr. 27, 2023, 4:15 PM), cnbc.com/2023/04/27/snap-q1-earnings-report-2023.html [https://perma.cc/YG5S-WD2W] ("Snap shares dropped as much as 20% after hours on Thursday as the company reported first-quarter results that

Understanding exactly why products like Facebook and Instagram have emerged from ATT comparatively stronger than a rival like Snapchat requires an in-depth examination of the online advertising business, how companies monetize data for advertising, and consequently the effects that ATT had on the industry.

Advertising is broadly divisible into two types: brand and direct response. The two categories operate on different time horizons. Brand advertising works on the long term: it raises awareness for the brand and seeks to instill affinity for the brand in consumers, all in the hopes that consumers will choose the brand when making a purchasing decision in the future.[262] Commercials for pickup trucks and beer that run during an NFL broadcast typify brand advertising.

In contrast, direct response seeks to elicit a decision from the viewer in the short term by prompting the audience to act quickly.[263] Traditional examples of direct-response advertising include QVC and late-night infomercials. During cable television's heyday, brand advertising reigned supreme and direct response was widely understood to be an exploitive backwater.[264]

The internet, however, injected new life into direct-response advertising. Rather than display a flashing telephone number onscreen while berating viewers to act fast, companies could display advertisements that users simply clicked or tapped. Clicking an online

missed analysts' expectations on revenue. . . . Like much larger rivals, including Facebook and Google, Snap continues to operate in a difficult online ad market in which companies have reduced their marketing and promotional spend as the economy remains shaky. But unlike those giant rivals, Snap doesn't have the enormous presence around the world to help manage the difficult digital ad sector more smoothly.").

[262] *See* Ben Thompson, *The Reality of Missing Out*, STRATECHERY (Feb. 9, 2016), stratechery.com/2016/the-reality-of-missing-out/ [https://perma.cc/N59U-FYEG] [hereinafter Thompson, *Missing Out*] (recounting traditional brand advertising techniques).

[263] *See* Ben Thompson, *Digital Advertising in 2022*, STRATECHERY (Feb. 8, 2022), stratechery.com/2022/digital-advertising-in-2022/ [https://perma.cc/W8AC-E56J] [hereinafter Thompson, *Digital Advertising*] (detailing digital direct response advertising techniques).

[264] *See, e.g.*, MIKE MORAN, DO IT WRONG QUICKLY: HOW THE WEB CHANGES THE OLD MARKETING RULES 15 (2007) ("Direct marketing. All marketers know what it is, but many of them treat direct marketing as a backwater inhabited by hucksters."); Thompson, *Missing Out*, *supra* note 262.

advertisement transports the user to an action space. Direct-response marketing on the internet is further subdivided into e-commerce and app installation.[265] Both seek an immediate action from the user, but e-commerce advertising prompts users to make an online purchase, whereas app-installation advertising prompts users to install an application — frequently, a free-to-play, pay-to-win mobile game.

Informational platforms like Facebook and Instagram are uniquely positioned to take advantage of direct-response marketing for at least three reasons: First, digital advertisements are interactive, shortening the time and effort required to take action. Second, feed-based advertising provided companies with an unprecedented ability to show different messages to different people. Third, companies gained access to an unparalleled volume of personal information to aid in the targeting of those unique commercial messages. Together, these changes allow informational platforms that sell advertising to create extremely sophisticated and precise targeting systems: companies collect vast amounts of social data and use that data to decide to whom to show advertisements; observing which users make decisions in response to particular advertisements becomes an extremely valuable input to the targeting regime.[266] And the simple reality is that it works: advertising on Facebook and Instagram generates more revenue than it costs.

ATT severed the attribution loop that had been critical to direct-response marketing: the companies that display advertisements lost the ability to know with certainty which users converted, that is, completed a purchase or installed an app.[267] Before ATT, Meta's platforms did not need to obtain consent to collect data from every stage of the advertising loop: they logged which users saw which ads, which users

[265] *See, e.g.*, Eric Silberstein, *App Tracking Transparency and eCommerce Ads*, KLAVIYO ENG'G (Mar. 3, 2022), klaviyo.tech/app-tracking-transparency-and-ecommerce-ads-4af3139a3916 [https://perma.cc/BN9E-F7WP] (explaining how ATT's technical implementation differs for app installs and e-commerce).

[266] *See, e.g.*, Eric Seufert, *The App Tracking Transparency Recession*, MOBILE DEV MEMO (Jan. 11, 2023), mobiledevmemo.com/the-att-recession/ [https://perma.cc/V8TJ-98MN] (detailing how this ad-targeting regime works).

[267] *See id.* ("ATT fundamentally prevents ad targeting at the level of an individual user: since user profiles cannot be developed through aggregated, user-level conversion data . . . then the user-level targeting mechanics previously employed by large platforms are rendered inoperable.").

clicked which ads, and which users converted by taking the desired action.[268] After ATT, the platforms lost — among other things — data from the third category: for those who opt out of tracking, the platforms cannot track which users convert off-platform.[269]

The loss of this measurement or conversion data is significant in its own right; platforms like Meta's lost visibility into the efficacy of any given advertising campaign, which drove down advertisers' willingness to pay for advertising of uncertain effectiveness.[270] But the loss was more significant still, since data about who converts is the single most important insight into who else is also most likely to convert.[271] Conversion data, for example, allows Meta to form detailed profiles of who has a high net worth and spends profligately on free-to-play pay-to-win mobile games.[272] So when a game developer turns to Meta's

[268] *See id.*

[269] *See id.*

[270] *See, e.g.*, Ben Thompson, *An Interview with Eric Seufert About the Post-ATT Landscape*, STRATECHERY (May 19, 2022), stratechery.com/2022/an-interview-with-eric-seufert-about-the-post-att-landscape/ [https://perma.cc/YCN7-D5H7] ("That's the measurement gap right now. It's just having the ability to tell an advertiser, you spent $1, you got a $1.10, or you spent $1 and you got 90 cents and they're all trying to fix that." (citing Graham Mudd, *Navigating Change and Improving Performance and Measurement*, META (Sept. 22, 2021), facebook.com/business/news/navigating-change-and-improving-performance-and-measurement [https://perma.cc/LL95-X3VC])); Goksu Nebol-Perlman, *Best Practices for More Accurate Reporting and Better Performance*, META (Feb. 14, 2022), facebook.com/business/news/best-practices-for-more-accurate-reporting-and-better-performance [https://perma.cc/X9DB-P9X4].

[271] *See* Seufert, *supra* note 266.

[272] This is not an outlandish hypothetical. The mobile game industry would not and could not exist in its current form without the ability to target wealthy and profligate players, which members of industry refer to as "whales." *See, e.g.*, Thompson, *supra* note 270 ("The entirety of the advertising ecosystem and especially when you get into apps in the freemium economy . . . [is] all driven by fat tails, by long tails. The . . . only way to monetize on the product level, but especially with the advertising level . . . is to be able to capture those high value people. Sometimes they're called whales, but those high value people that want to spend a lot of money, and you offer them the ability to spend a lot of money, the only way to make the economics work is capture them, because most of the time people spend zero. A lot of your impressions are wasted, because people just aren't ready to spend money. So the only way to make these model work is a bottoms-up approach. 'I'm going to find those people specifically, I'm going to find those individuals' and when you have to go to group level, there's just so much loss, so much inefficiency, that the economics can become impossible."). The CEO of Match Group,

advertising tools to find additional high-value players, it need only provide the platform with its marketing assets and budget, and Meta's advertising targeting system goes out, tests those assets against different users, and finds the most lucrative audience — ultimately displaying the developer's campaign in those users' custom feeds.[273]

ATT does not affect two closely related types of businesses: those that display advertising on the web and those where conversions occur on-platform. In the former's case, Apple cannot use the threat of removal from the App Store to ensure compliance, since the web is cross-platform, operating across devices in a way that the iOS App Store does not.[274] In the latter's case, there has been no cross-site tracking: if an online retailer displays an advertisement, a user clicks it, and then the user completes a purchase, everything has occurred on the retailer's own platform.[275]

for example, admitted that he'd spent $50,000 in three months to build a wall in Clash of Clans. Mitchell Clark, *Match Group's CEO Says He Spent $50K in Three Months on Clash of Clans*, THE VERGE (Mar. 15, 2023, 6:46 PM), theverge.com/2023/3/15/23642400/match-ceo-50000-clash-of-clans-tinder [https://perma.cc/PN6P-EQG4] ("I've personally spent $50,000 in three months in Clash of Clans, and I still look back at that with lots of shame. I'm like 'oh my God, what did I really get out of that experience?' Nothing, other than, like, a really amazing wall . . . .").

[273] *See How to Create a Lookalike Audience on Meta Ads Manager*, META, facebook.com/business/help/465262276878947 (last visited Oct. 11, 2023) [https://perma.cc/TFF2-MCQ2]; Thompson, *supra* note 174; Ben Thompson, *Privacy Labels and Lookalike Audiences*, STRATECHERY (Dec. 8, 2020), stratechery.com/2020/privacy-labels-and-lookalike-audiences/ [https://perma.cc/CUS8-G389].

[274] *See, e.g.*, Seufert, *supra* note 266 ("Google Search is observably exempt from the restrictions of ATT because Google Search is primarily conducted in a browser, and Google Search results are primarily delivered as a result of search queries and first-party, on-site data."); Thompson, *Digital Advertising*, *supra* note 263 (quoting Meta CFO Dave Wehner) ("[W]e believe those restrictions from Apple are designed in a way that carves out browsers from the tracking prompts Apple requires for apps. And so what that means is that search ads could have access to far more third-party data for measurement and optimization purposes than app-based ad platforms like ours.").

[275] *See, e.g.*, Thompson, *Digital Advertising*, *supra* note 263 ("Amazon also has data on its users, and it is free to collect as much of it as it likes, and leverage it however it wishes when it comes to selling ads. This is because all of Amazon's data collection, ad targeting, and conversion happen on the same platform — Amazon.com, or the Amazon app. ATT only restricts third party data sharing, which means it doesn't affect Amazon at all.").

This disparate application of ATT provides a stark natural experiment. The advertising businesses of Google Search (web) and Amazon (on-platform) were mostly untouched by ATT, whereas the businesses of Facebook, Instagram, YouTube, and Snapchat were directly implicated:

> Every company that relies on performance marketing, from Snap to YouTube to Meta to Shopify has seen its revenue growth crash from the moment ATT came into force in late 2021, even as companies and products that were isolated from its effects, from Amazon to Google to Apple advertising has seen growth.[276]

Concretely, the growth of Meta's advertising revenue and price per ad fell precipitously beginning in 2021 and more significantly in 2022.[277] While Meta's advertising business faced numerous headwinds at this time — increasing competition from TikTok, a post-pandemic hangover, and broader macroeconomic conditions — industry insiders agree that ATT was a significant contributor to the company's struggles.[278] Snap's advertising business has been decimated over the

[276] Ben Thompson, *The Four Horsemen of the Tech Recession*, STRATECHERY (Feb. 6, 2023), stratechery.com/2023/the-four-horsemen-of-the-tech-recession/ [https://perma.cc/8D4T-ACP8].

[277] *See, e.g.*, Needleman, *supra* note 260 (documenting Meta's slowing ad sales in the first quarter after ATT took effect); Bobrowsky, *supra* note 259 (documenting Meta's forecast that ATT would cost it $10 billion in lost ad sales for 2022); Ben Thompson, *Meta Earnings, Meta Spending, AI Costs and Moats*, STRATECHERY (Apr. 28, 2022), stratechery.com/2022/meta-earnings-meta-spending-ai-costs-and-moats/ [https://perma.cc/GH3C-VWJ9] (documenting the growth rates of Meta's impressions, daily active users, price per ad, and advertising revenue from 2016 to 2022 in chart form); *see also* 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 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4698374 [https://perma.cc/QU3L-4AV7] ("We show that the performance of conversion-optimized Meta advertisements, which critically depend on third-party data for targeting and measurement, significantly worsened after ATT with a 37% reduction in click-through rates compared to click-optimized campaigns.").

[278] *See, e.g.*, Seufert, *supra* note 266 ("Apple's App Tracking Transparency (ATT) privacy policy . . . has created a recession within the social media advertising economy and certain other advertising-dependent categories."); Thompson, *Digital Advertising*, *supra* note 263 ("App Tracking Transparency (ATT) initiative severed the connection

same period, and the company — despite ill-founded initial optimism — has slowly realized how profoundly ATT has crippled its business.[279]

YouTube is another service that has traditionally had a robust direct-response business — app-install ads specifically.[280] And like Meta and Snap, YouTube's direct-response business suffered an outsized downturn throughout 2022.[281] To be clear, Google Search also

amongst e-commerce sellers, app developers, and Facebook by which Facebook achieved that ROI, and while the company is better positioned than anyone else to build a replacement, it is important to note that the impairment entailed in probabilistically measuring ad effectiveness instead of deterministically is a permanent one. . . . There is no question that Facebook has been significantly impaired, but the company is by no means doomed . . . .").

[279] *See* Sarah E. Needleman, *Snap's Stock Plummets as It Blames Apple's Privacy Changes for Hurting Its Ad Business*, WALL ST. J. (Oct. 21, 2021), wsj.com/articles/snap-blames-apples-privacy-changes-for-hurting-its-ad-business-11634847647; Meghan Bobrowsky, *Snap Issues Profit Warning on Economic Conditions Including Inflation*, WALL ST. J. (May 23, 2022), wsj.com/articles/snap-issues-profit-warning-on-deteriorating-macroeconomic-environment-11653341398; Chelsey Dulaney, *Snap Stock Tumbles as Digital-Advertising Concerns Spread*, WALL ST. J. (July 22, 2022), wsj.com/articles/snap-shares-tumble-as-digital-advertising-concerns-spread-11658502221; Alex Barinka, *Snap Plunges on Slowest Sales Growth as Advertisers Retreat*, BLOOMBERG (Oct. 20, 2022), bloomberg.com/news/articles/2022-10-20/snap-falls-on-slow-sales-growth-as-advertisers-pull-back [https://perma.cc/S65N-5PT7]; Vanian, *supra* note 261; Taylor Hatmaker, *Snap's Revenue Woes Continue But Earnings Yield a Few Bright Spots*, TECHCRUNCH (July 25, 2023, 2:50 PM), techcrunch.com/2023/07/25/snap-snapchat-q2-2023-earnings/ [https://perma.cc/72G8-WPHV]; Jonathan Vanian, *Snap Shares Plunge More Than 20% on Weak Guidance*, CNBC (Aug. 1, 2024, 4:14 PM), https://www.cnbc.com/2024/08/01/snap-shares-plunge-over-20percent-af.html [https://perma.cc/PD8N-FVZA]; *see also* Ben Thompson, *An Interview With Eric Seufert About the Future of Digital Advertising*, STRATECHERY (Aug. 18, 2022), stratechery.com/2022/an-interview-with-eric-seufert-about-the-future-of-digital-advertising/ [https://perma.cc/YC5Y-67YU] (discussing Snap's "disastrous" year and its seeming confusion over ATT's effects); Yiwen Lu, *Snap Shares Plummet After First-Quarter Guidance Disappoints*, N.Y. TIMES (Feb. 6, 2024), nytimes.com/2024/02/06/technology/snap-earnings.html.

[280] *See* Thompson, *supra* note 263 ("In terms of ATT, it is notable that the only part of Google's business that fell short of Wall Street expectations was YouTube; I suspect it is not a coincidence that YouTube has a significant app-install business of its own, and ATT's restrictions on what those installed apps can report back to Google may have hurt business a bit.").

[281] *See* Ben Thompson, *Twitter Follow-Up, Google Earnings, ATT and Google*, STRATECHERY (Apr. 27, 2022), stratechery.com/2022/twitter-follow-up-google-earnings-att-and-google/ [https://perma.cc/QZV4-22VY]; Ben Thompson, *Google Earnings, YouTube Growth Strategies, Shopify Layoffs and Earnings*, STRATECHERY (July 27, 2022),

experienced slowing revenue over the same period, but before ATT, YouTube was growing faster than Search, and after ATT, YouTube's growth has underperformed Search.[282]

The explosion of Amazon's advertising business supplies additional corroboration. Amazon first reported its advertising revenue for the last three months of 2021: $9.7 billion in revenue, a thirty-two percent increase year-over-year.[283] For comparison, in the same quarter, Google reported $61.2 billion, Meta reported $32.6 billion, and Snap reported $1.3 billion.[284] Ever since, Amazon's advertising growth has remained robust.[285] Amazon's advertising success is attributable at least in part to the fact its business is mostly exempt from ATT: "Amazon . . . is free to collect as much [data] as it likes, and leverage it however it wishes when it comes to selling ads. This is because all of Amazon's data collection,

stratechery.com/2022/google-earnings-youtube-growth-strategies-shopify-layoffs-and-earnings/ [https://perma.cc/AN9U-DCCA] (quoting Eric Seufert (@eric_seufert), Twitter (July 26, 2022, 8:53 PM), web.archive.org/web/20220726205427/https://twitter.com/eric_seufert/status/1552034298244567040 [https://perma.cc/W2EY-MZGX]); Ben Thompson, *Google Earnings, Gaming's Warning Light, Google's Costs*, STRATECHERY (Oct. 26, 2022), stratechery.com/2022/google-earnings-gamings-warning-light-googles-costs/ [https://perma.cc/PK4W-66VU]; Ben Thompson, *Google Earnings, YouTube's Aggregation Bid, YouTube Shorts Monetization*, STRATECHERY (Feb. 7, 2023), stratechery.com/2023/google-earnings-youtubes-aggregation-bid-youtube-shorts-monetization/ [https://perma.cc/8SPY-LJ5G].

[282] *See* Seufert, *supra* note 266 ("[B]oth YouTube and Search see year-over-year growth decline from a peak in Q2 2021. . . . But YouTube's year-over-year growth rate slows more dramatically than Search's after ATT reaches majority scale in Q2 2021 . . . . If a reversion to post-COVID behavioral norms explains the decline in Search revenue starting in Q2 2021 . . . , then my assertion is that ATT explains the more aggravated decline in growth in YouTube relative to Search.").

[283] Thompson, *Digital Advertising*, *supra* note 263.

[284] *Id.*

[285] *See* Jonathan Vanian, *Amazon's Online Advertising Unit just Brought in Over $10 Billion in the Second Quarter*, CNBC (Aug. 3, 2023, 4:10PM), cnbc.com/2023/08/03/amazon-online-advertising-unit-just-brought-in-over-10-billion-in-q2.html [https://perma.cc/VQV8-MDA9]; Press Release, Amazon, Amazon.com Announces Fourth Quarter Results (Feb. 1, 2024), ir.aboutamazon.com/news-release/news-release-details/2024/Amazon.com-Announces-Fourth-Quarter-Results/ [https://perma.cc/9Q8F-VXPZ].

ad targeting, and conversion happen on the same platform — Amazon.com, or the Amazon app."[286]

These core dynamics — a decline in direct-response advertising effected by ATT, but little sign of advertising downturns elsewhere — continued throughout 2023 — with one notable exception. In early 2023, Meta's fortunes abruptly reversed.[287] At the same time its advertising revenue returned to growth, its executives touted the progress they had made in measuring conversions.[288] Slowly but surely, the company has clawed back the precision of its measurement tools through the use of machine-learning and artificial-intelligence techniques.[289] In short, Meta has adapted to the post-ATT environment by honing its ability to model the efficacy of its direct-response advertising.

The difference between Meta and its direct-response competitors illustrates the power to circumvent: if your company is big enough and your predictive analytics are sophisticated enough, even the most stringent consent-based privacy rules will not meaningfully affect your business in the long term.[290] To be clear, ATT irrevocably ends deterministic measurement of advertising conversions for those who opt out of tracking. But Meta has proven wildly successful in responding to that loss by creating an almost-as-good probabilistic model of conversion and targeting. They continue to be unable to say with certainty which users converted, but their machine-learning and artificial-intelligence models get them close enough that it doesn't seem to matter.

---

[286] Thompson, *supra* note 263.

[287] *See* Rodriguez, *supra* note 261; Ben Thompson, *Facebook Earnings, Generative AI and Messaging Monetization, Open Source and AI*, STRATECHERY (May 3, 2023), stratechery.com/2023/facebook-earnings-generative-ai-and-messaging-monetization-open-source-and-ai/ [https://perma.cc/LQ5W-TQ8C].

[288] *See* Meta Platforms, Inc., *Transcript of First Quarter 2023 Results Conference Call* (Apr. 26, 2023), s21.q4cdn.com/399680738/files/doc_financials/2023/q1/META-Q1-2023-Earnings-Call-Transcript.pdf [https://perma.cc/9ZJL-MYLD] ("[W]e believe our ongoing improvements to ad targeting and measurement are continuing to drive improved results for advertisers.").

[289] *See* Thompson, Feb. 2023 Interview, *supra* note 174.

[290] Concretely, as of August 2024, Meta's share price has increased since ATT's implementation by about seventy percent. In contrast, Snap's share price has declined over the same period by over eighty-five percent.

In fairness, ATT did reduce advertising efficacy across the board. But advertisers' budgets ultimately must go somewhere, and the power to circumvent illustrates that the companies with the most data will increasingly be the first and best choice for those advertising dollars. Suppose you're the game developer with that free-to-play pay-to-win game, and you must choose where to spend your marketing budget to obtain the most high-value players. Perhaps Meta's advertising is less effective than it was four years ago, but it has proven to be far more effective than its competitors.

While ATT provides a stark illustration of the power to circumvent, the dynamic is not limited to this single initiative. Google's similar effort to eliminate third-party cookies from Chrome has attracted scrutiny from the United Kingdom's competition regulator.[291] Empirical research has found that eliminating other forms of tracking ultimately ends up benefiting the biggest companies with the most data.[292] Privacy restrictions that revolve around consent therefore incentivize the so-called "content fortress": a "platform or portfolio of products supported by a rich advertising ecosystem serving owned and operated inventory using only first-party data."[293] First-party data becomes essential when consent to "tracking" is limited or withheld, since using first-party data in advertising measurement and targeting doesn't meet the widely accepted definition of "tracking."[294] This has helped spur a race to agglomerate as much first-party data as possible, leading to consolidation in the ad-tech and mobile-gaming sectors in particular.[295]

---

[291] *See Update on the Plan for Phase-Out of Third-Party Cookies on Chrome*, GOOGLE (Apr. 23, 2024), privacysandbox.com/intl/en_us/news/update-on-the-plan-for-phase-out-of-third-party-cookies-on-chrome/ [https://perma.cc/3VY3-Y76M]; Eric Seufert, *Why Is Google killing Cookies?*, MOBILE DEV MEMO (Feb. 19, 2024), mobiledevmemo.com/why-is-google-killing-cookies/ [https://perma.cc/Y58Z-Q7MN].

[292] *See* Miguel Alcobendas, Shunto J. Kobayashi, Ke Shi & Matthew Shum, *The Impact of Privacy Measures on Online Advertising Markets* (Oct. 6, 2023), ssrn.com/abstract=3900215 [https://perma.cc/DJ4M-9MJN].

[293] Eric Seufert, *Content Fortresses and the New Privacy Landscape*, MOBILE DEV MEMO (July 12, 2021), mobiledevmemo.com/content-fortresses-and-the-new-privacy-landscape/ [https://perma.cc/EP9G-ZGJT].

[294] *See id.*

[295] *See id.*; *see, e.g.*, Ben Thompson, *Gaming the Smiling Curve*, STRATECHERY (Feb. 1, 2022), stratechery.com/2022/gaming-the-smiling-curve/ [https://perma.cc/K35V-T66P]

It has also compelled platforms like Meta to move as much conversion on-platform as possible, further consolidating their business and raising the walls of their garden.[296] And a company of Meta's scale has similarly become an attractive partner for Amazon's fulfillment network, another advantage unavailable to smaller rivals.[297] New privacy rules make scale a competitive advantage, and that necessitates consolidation and centralization — ultimately reducing the number of competitors.

In sum, even stringent and widely exercised consent-based privacy rules confer an advantage on the biggest companies. Upstarts cannot account for the data losses, whereas incumbents with sufficient scale are uniquely capable of honing techniques to infer around the lost data. The power to circumvent therefore shows that the advantages of incumbency are not coterminous with weak and ineffective consent rules — rather, the stronger the consent-based rule, the more dominant companies benefit.

***

Suppose for a moment that Congress eventually enacts an omnibus privacy law, like the American Data Privacy and Protection Act or something materially similar. The bill is modeled on the GDPR and CCPA: it defines "covered entities" and "covered data" broadly; it primarily confers on individuals a host of informational rights, like access, correction, deletion, and portability; it adopts an opt-out

("ATT, meanwhile, didn't ban data collection or analysis or targeting or any of the other aspects of advertising that many of its supporters object to; what it targeted was doing so collectively. That means that the policy has been a huge boon for fully integrated advertisers (i.e.[,] advertisers that collect data, target, and show advertisements) like Google and Amazon. In this world the natural response has been consolidation . . . ."). *See generally* Maor Sadra, *Why is AdTech Hot Again?*, MOBILE DEV MEMO (June 10, 2021), mobiledevmemo.com/is-adtech-hot-again/ [https://perma.cc/G8Y9-C8L4] (identifying ATT as the reason for "a plethora of acquisitions" in the advertising tech industry).

[296] *See* Ben Thompson, *Shopify-Amazon Follow-Up, Amazon and Pinterest, Meta Shops to Require Native Checkout*, STRATECHERY (May 9, 2023), stratechery.com/2023/shopify-amazon-follow-up-amazon-and-pinterest-meta-shops-to-require-native-checkout/ [https://perma.cc/UTA9-5BP3].

[297] *See* Spencer Soper & Aisha Counts, *Amazon Allies with Meta for Shopping via Instagram, Facebook*, BLOOMBERG (Nov. 9, 2023, 10:31 AM PST), bloomberg.com/news/articles/2023-11-09/amazon-and-facebook-partner-on-new-app-based-shopping-feature [https://perma.cc/L9WX-4QNF].

approach to most information collection and processing; and it imposes a host of transparency obligations and other informational duties on covered entities.[298] It vests most enforcement authority with the FTC, though it contains a limited private right of action in exchange for broad preemption of state privacy laws.[299]

How would the powers of incumbency manifest in a world where something similar became law? The bill does impose more stringent disclosure, certification, and audit requirements on entities like search engines and social media networks, but its expansive definitions and coverage mean that companies both large and small must comply with most of its provisions. Incumbents will realize economies of scale in repurposing their bespoke in-house CCPA and GDPR compliance regimes, whereas upstarts will turn to third-party vendors for compliance solutions. When it comes to obtaining consent, entrenched incumbents will have little difficulty continuing to obtain user data, while insurgents will have more difficulty convincing users of their value proposition. Companies of all sizes will need to design materially identical opt-out and rights-assertion software experiences, though large companies will be able to spread those costs across their enormous user bases. The law's passage will cast a pall over many data-sharing initiatives and provide companies with pretextual bases for buttoning down the hatches and resisting transparency initiatives and competition mandates. Once implemented, companies will point to the law's opt-out provisions and their own terms of service to prevent competitors from collecting even publicly available data. And over time, restrictions on data collection and processing will prove most deleterious to the smallest companies with the least data, while the largest companies will keep honing their probabilistic models to infer around data losses attributable to the law. Together, the new statute may ratchet up privacy protections for the vanishing minority of users motivated to assert — and keep asserting — their privacy rights, but the engine of surveillance value-extraction will churn on mostly unencumbered. And in exchange for that dubious tradeoff, social data's value will disproportionately flow

[298] *See* JONATHAN M. GAFFNEY, ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (updated Aug. 31, 2022), crsreports.congress.gov/product/pdf/LSB/LSB10776.

[299] *See id.*

to the biggest companies, allowing them to further consolidate their power and brush back emerging threats to their dominance.

The past half-decade has witnessed a wave of new privacy restrictions; in the European Union, in statehouses, and in private-sector initiatives. These initiatives and Congressional proposals they've inspired may differ at the margins, but they all share a common denominator: empowering individuals to exercise individual privacy rights. The effect these changes have had on competition in digital markets has only been studied in a limited way, but this Part has furthered that effort by identifying three distinct powers that consent-and-control privacy rules confer on the biggest and most dominant firms: compliance, restriction, and circumvention.

IV. LESSONS

In light of privacy law's penchant for conferring advantages on the biggest companies, this Part considers lessons that commentators and policymakers should internalize, and it raises follow-on questions for further research. Part IV.A addresses two salient lessons for antitrust law: that policymakers should be wary about using competition to address privacy problems and that pro-competition policy responses will prove deleterious to privacy. Part IV.B turns to privacy law — arguing that the consent-and-control paradigm bears responsibility for advantaging incumbents and suggesting an alternative approach.

A. For Antitrust Law

There are two salient lessons for competition law. The first addresses the impulse to favor competition over privacy. The second reviews the implications of policy responses that promote competition.

1. Competition's Limits

Policymakers should be wary of reductive arguments that competition will solve privacy problems.

The integrationists posit, as detailed in Part II.B, that greater competition produces greater privacy protections, since privacy is a non-price product-quality parameter that is itself a site of competitive pressure between firms. On the other hand, Part III has detailed that

increased privacy mandates favor dominant firms. In light of these two dynamics, the argument goes, shouldn't policymakers who wish to achieve both privacy and competition always choose to maximize competition? After all, greater competition increases privacy, whereas legislating privacy reduces competition.

Despite the allure of this syllogism, there are good reasons for questioning its validity. The integrationists' illustrations (e.g., Meta's post-acquisition degradation of WhatsApp's privacy protections, the existence of DuckDuckGo, and so forth) do not support the strong version of the first premise — that more competition will inevitably produce greater privacy options. It is by no means self-evident that more competition will always necessarily produce more privacy, and the privacy that competition produces is of dubious quality.

Jeffrey L. Vagle has explained that "it is difficult to see how increased competition will necessarily lead to increased protections for information privacy," because while dominant technology companies left unchallenged "will have little incentive to introduce or increase privacy protections, even when firms compete on privacy, users are often at a significant information deficit as to exactly what particular privacy protections mean in real terms."[300] Policymakers hoping that antitrust remedies like breakups will spur competition for privacy must confront the fact "there is little to no evidence that these newer, smaller companies would do anything more to protect user privacy, even if the breakup had nominally increased competition."[301]

It is of course possible that players in a newly competitive digital market will seek to distinguish themselves by promising consumers greater privacy protections, but that result is not self-evident and hardly ensures meaningful differences on the ground. After all, cost pressure in a fiercely competitive market may trigger a race to the bottom wherein companies engage in ever-more exploitive and invasive data processing to gain a competitive edge. The television manufacturer Vizio, for example, makes twice as much money on its customers' data as it does

[300] Jeffrey L. Vagle, *Privacy's Commodification and the Limits of Antitrust*, 77 ARK. L. REV. 51, 116 (2024).

[301] *Id.* at 123.

on the television sales themselves,[302] and customers have documented how their Vizio televisions communicate with servers nearly every second of every day.[303] When prompted, Vizio's CTO argued that the competitiveness of the industry justified their surveillance subsidy.[304] The uncomfortable reality is that there are many more companies like Vizio than like DuckDuckGo, and even companies that profess privacy bonafides cast them aside when their investors demand it.[305]

There is, moreover, no real impediment to obscuring these realities with vague pro-privacy representations.[306] This tendency of tech

[302] *See* Richard Lawler, *Vizio's Profit on Ads, Subscriptions, and Data is Double the Money it Makes Selling TVs*, THE VERGE (Nov. 10, 2021, 10:12 AM PST), theverge.com/2021/11/10/22773073/vizio-acr-advertising-inscape-data-privacy-q3-2021 [https://perma.cc/7T24-8CQU]; *see also, e.g.*, Chris Welch, *Roku is in the Ad Business, Not the Hardware Business, Says CEO*, THE VERGE (July 20, 2018, 10:30 AM PDT), theverge.com/2018/7/20/17595384/roku-ceo-anthony-wood-ads-hardware-business-interview-business-model [https://perma.cc/YJU2-U4ED] (quoting Roku's CEO as explaining, "We . . . certainly don't make enough money to support our engineering organization and our operations and the cost of money to run the Roku service. . . . That's not paid for by the hardware. That's paid for by our ad and content business.").

[303] *See, e.g.*, *Vizio M Series TV was Sending 80,000 Requests per Day, Discovered and Fixed Thanks to Pi-Hole*, REDDIT (2020), reddit.com/r/pihole/comments/jlt7rx/vizio_m_series_tv_was_sending_80000_requests_per/ [https://perma.cc/TS5R-GEDQ] (documenting a Vizio television making 80,000 requests per day).

[304] *See* Nilay Patel, *Taking the Smarts Out of Smart TVs Would Make Them More Expensive*, THE VERGE (Jan. 7, 2019, 4:46 PM PST), theverge.com/2019/1/7/18172397/airplay-2-homekit-vizio-tv-bill-baxter-interview-vergecast-ces-2019 [https://perma.cc/4YR5-8LPA] ("This is a cutthroat industry. It's a 6-percent margin industry, right? I mean, you know it's pretty ruthless.").

[305] *Cf.* Casey Newton, *The Ad Model is Coming to AI*, PLATFORMER (Apr. 1, 2024), platformer.news/perplexity-ai-ads-privacy-risks [https://perma.cc/CM7R-VW63] ("[Perplexity's] own about page said 'Perplexity was founded on the belief that searching for information should be a straightforward, efficient experience, free from the influence of advertising-driven models.' As of today, that sentence has been quietly edited to remove the final clause.").

[306] Vizio's CTO illustrates the point when, asked about his products' perpetual surveillance, he replied, "I think you know that Vizio has been pioneering privacy and active viewing data disclosures for the last several years, and we actually lead the industry in those disclosures." Patel, *supra* note 304. Vizio paid a $2.2 million fine to the FTC in 2017 for collecting its customers' viewing histories without consent. *See* Press Release, Fed. Trade Comm'n, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), ftc.gov/news-events/news/press-releases/2017/02/vizio-

companies to rely on meaningless incantations like, "Your privacy is important to us," lends support to this darker characterization of the market for privacy.[307] Because technology companies today are reliant on the surveil-for-profit model, and because the realities of their data practices are easily obscured and poorly understood, the competitive pressure is to *appear* sensitive to privacy concerns rather than actually pursuing a difference in substance.[308] "Privacy competition," in other words, "becomes a shell game of semantics, confusing consumers at best, and at worse, creating generations of privacy nihilists."[309] To collapse the divide between companies' privacy representations and their actual privacy practices would require a vast reimagining of what constitutes deception and who is empowered to seek redress for it.[310] While it may be an anathema to some antitrust scholars, it is hard to resist the conclusion that competition is no panacea.[311]

Such a pessimistic view of the benefits of greater competition may seem striking. After all, Part III argued at length that privacy law is advantaging incumbents — with the implication being that greater competition would be preferable. You might then wonder, in light of pessimism about competition's capacity to solve privacy problems, in

pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million [https://perma.cc/GX57-S95N].

[307] *See* Waldman, *supra* note 185, at 196 (critically reviewing technology companies' vague pro-privacy representations).

[308] *See* Vagle, *supra* note 300, at 72-88. Microsoft's surveillance backdoor to DuckDuckGo is a further illustration of this dynamic. *See* Chen, *supra* note 122, at 565. And in a related vein, empiricists have found that firms who tout their diversity, equity, and inclusion initiatives realize significant financial upside even when their actual practices on the ground are inconsistent with their messaging. *See* Andrew C. Baker, David F. Larcker, Charles G. McClure, Durgesh Saraph & Edward M. Watts, *Diversity Washing*, J. ACCT. RSCH. (Apr. 25, 2024), doi.org/10.1111/1475-679X.12542 [https://perma.cc/8Q36-7GEC].

[309] Vagle, *supra* note 300, at 124.

[310] *See, e.g.*, Myriam Gilles & Gary Friedman, *The New Qui Tam: A Model for the Enforcement of Group Rights in a Hostile Era*, 98 TEX. L. REV. 489, 491 (2020) (proposing a qui tam enforcement scheme in light of little agency enforcement); Ormerod, *supra* note 50, at 282-89 (proposing a qui tam enforcement scheme to address under-enforcement).

[311] *Cf.* Sipe, *supra* note 18, at 398-99 ("[A]n increase in the number of market competitors may not necessarily yield an increase in consumer privacy. With respect to Big Tech in particular, there are many reasons to suspect it would actually cause the opposite outcome.").

what sense is privacy law creating an incumbency "problem" at all? Why should we care that privacy law is inhibiting competition?

Policymakers should be concerned about privacy law's tendency to advantage incumbents not because consumers will suffer from a lack of choice but because of the threats posed by the concentration of power over the information economy. Policymakers and commentators have long identified a diverse panoply of risks associated with concentrated control over the critical inputs to twenty-first-century prosperity: from swaying elections[312] and national-security concerns,[313] to unique threats to youths[314] and labor-market distortions.[315] Such enormously large and wealthy firms cannot be meaningfully governed. After all, the FTC's $5 billion settlement with Facebook in 2019 shattered records, but the fine represented only a month of the company's earnings at the time.[316] And in the five years since, the company has only become wildly more

[312] *See, e.g.*, Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 UC DAVIS L. REV. 1183, 1188-89 (2016) (discussing Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/5KBA-KEXV]).

[313] *See, e.g.*, Sapna Maheshwari & Amanda Holpuch, *Why the U.S. Is Forcing TikTok to Be Sold or Banned*, N.Y. TIMES (Apr. 26, 2024), nytimes.com/article/tiktok-ban.html ("Concerns that the Chinese government could access sensitive user data through the short-form video app TikTok, which is owned by the Chinese company ByteDance, have prompted the U.S. government to pass legislation banning the social media platform unless it is sold to a government-approved buyer.").

[314] *See, e.g.*, Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM EST), wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 ("For the past three years, Facebook has been conducting studies into how its photo-sharing app affects its millions of young users. Repeatedly, the company's researchers found that Instagram is harmful for a sizable percentage of them, most notably teenage girls.").

[315] *See, e.g.*, ERIC A. POSNER, HOW ANTITRUST FAILED WORKERS 1-7 (2021) (articulating the book's thesis that increased concentration has artificially suppressed wages).

[316] *See* Cohen, *supra* note 48.

profitable.[317] For the biggest tech companies, consumer-protection compliance "is little more than a necessary cost of doing business."[318]

Enacting privacy laws that further consolidate digital-market power is ultimately then self-defeating: any gains to individuals' privacy — itself a questionable outcome — are offset by further entrenching, enriching, and empowering the same companies whose business practices threaten a host of public imperatives, including privacy.

2. Policy Responses

Pro-competition policy responses to the three incumbency advantages detailed in Part III will tend to make privacy problems worse.

A plausible reaction to the powers of incumbency detailed in Part III is to suggest that pro-competition policies should be enacted in concert with pro-privacy policies. But a closer examination suggests that attempts to counteract incumbency's advantages will undermine the privacy rules responsible for conferring the advantage.

One response to the power to comply is to limit privacy-protecting rules to only the largest companies. The CCPA, for example, applies only to for-profit companies that have a gross annual revenue over $25 million; that buy, sell, or share the personal information of 100,000 or more California residents; or that derive more than half their annual revenue from selling California residents' personal information.[319] Applicability discrepancies like this surely do lessen the compliance burden on smaller entities, but they come at the cost of privacy protections for anyone whose information is collected and processed by smaller entities. Small medical practices, for example, are not exempt

[317] *See* Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend, (Feb. 1, 2024), investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx [https://perma.cc/TW69-EE42] (reporting $40 billion in revenue and $14 billion in profit for the last three months of 2023).

[318] Ormerod, *supra* note 50, at 272, 289-92.

[319] *See* CAL. CIV. CODE § 1798.140(d).

from health privacy rules.[320] Size-based coverage cutoffs also invite gamesmanship into remaining under the triggering threshold.[321]

An alternative that holds more promise is a tax-and-subsidy regime for compliance efforts. Under such an approach, large tech companies would be subject to taxation that would fund subsidies for smaller companies' compliance efforts. A tax-and-subsidy compliance program has its own difficulties, however — namely, tax law's limited ability to account for value creation in the information economy.[322]

A pro-competition response to the power to restrict would likely focus on prying open large companies' incentives to and practices of enclosing their platform ecosystems. To combat incumbents' tendency to restrict competitors' access to their data, competition law might impose a duty to deal to digital markets. There is no duty to deal under current law, and some competition scholars have argued that antitrust reforms should impose interoperability and other obligations on dominant platforms.[323] A more targeted alternative could draw an analogy to compulsory licenses under the Copyright Act, supplying smaller competitors with a legal basis for licensing data from dominant incumbents.[324] Alas, while these reform proposals would likely improve competition, by virtue of opening data flows, they necessarily undercut privacy law.

Finally, there are few pro-competition responses to the power to circumvent. In response to industry's outcry over ATT's data loss, Apple

---

[320] *See* 45 C.F.R. § 160.103 (defining "covered entity" for purposes of the HIPAA Privacy Rule).

[321] *Cf.* Natasha Lomas, *Europe Names 19 Platforms that Must Report Algorithmic Risks Under DSA*, TECHCRUNCH (Apr. 25, 2023, 8:38 AM CST), techcrunch.com/2023/04/25/europe-names-19-platforms-that-must-report-algorithmic-risks-under-dsa/ [https://perma.cc/66V3-GLP4] (enumerating the DSA's VLOPs); Samuel Stolton, *Apple Set to Avoid EU Crackdown Over iMessage Service*, BLOOMBERG (Dec. 6, 2023, 2:53 AM), bloomberg.com/news/articles/2023-12-06/apple-imessage-set-to-avoid-eu-s-digital-dominance-crackdown (documenting that iMessage isn't covered under the DMA because it is not popular enough with business users).

[322] *See* Parsons & Viljoen, *supra* note 225, at 1059-61.

[323] *See, e.g.*, Erik Hovencamp, *The Antitrust Duty to Deal in the Age of Big Tech*, 131 YALE L.J. 1483, 1524-38 (2021) (advocating for a lower standard of judicial scrutiny to govern some exclusionary refusals to deal).

[324] *See* 17 U.S.C. § 115.

has improved the quality and quantity of attribution data it makes programmatically available to app developers.[325] It is not hard to imagine a privacy-sensitive competition mandate would attempt to do something similar — requiring that aggregated and anonymized data be shared to aid competition. It is not clear such a mandate would or could be successful. Initial reports suggest that the companies capable of making the most of Apple's privacy-protecting attribution data are the biggest ones.[326] At least some of Meta's progress in responding to ATT, in other words, is thanks to Apple making more data available. Meta is already armed with a vast amount of data: from the pre-ATT era, from Android users, from users that opt in to tracking, from on-platform conversions, and from other sources.[327] Privatized attribution data gives a company of Meta's scale another input to further develop and refine an already sophisticated probabilistic model. Smaller companies, as we've already seen, have not been able to make similar progress — suggesting that even attempts to sand off the sharpest edges of privacy-inspired data losses will ultimately benefit incumbents.

European regulators and commentators are most attuned to the tension between competition and privacy, and the recent enactment of the Digital Markets Act and Digital Services Act are at least partially responses to the GDPR.[328] Whether the European approach — pairing an omnibus privacy law with more targeted competition mandates — will successfully protect privacy without advantaging incumbents is difficult to know at this juncture, given how new the laws are and how slowly enforcement in Europe proceeds.[329]

---

[325] *See* Thompson, Feb. 2023 Interview, *supra* note 174.

[326] *See id.* ("[Apple's] SKAdNetwork 4.0 is more signal, right? It's more data to latch onto. It's more data to feed into the machine. And who's got the best machine? I think that could be another bull case to be made for the biggest platforms.").

[327] *See* Thompson, May 2023 Interview, *supra* note 174.

[328] *See* Mackrael & Schechner, *supra* note 187.

[329] It's of course possible that the European approach — pairing a widely applicable data protection regulation with tailored competition measures — will prove successful at providing individual control rights without advantaging dominant incumbents. While the GDPR's capacity for giving users *meaningful* control over their information is contestable and contested, *see* Part I.B, it is too soon to know what effect the DMA will have on competition, and the DMA has a long road ahead to mitigate the GDPR's effects on competition. *See generally* Geradin, *supra* note 179, at 90-92 (proposing strategies for

B. For Privacy Law

The tug of war between competition and privacy does not only bode poorly for antitrust law. Privacy law today — and specifically the widespread reliance on the consent-and-control paradigm — is ill-equipped to achieve its stated ends, while at the same time it entrenches and thereby benefits the market actors who most seriously threaten privacy. Clarity about the consent-and-control paradigm's role in the powers of incumbency suggests a different path for privacy law.

1. Consent's Culpability

The penchant of the consent-and-control approach for benefiting incumbents raises troubling questions about the efficacy of prevailing notions of "privacy law" and the extent to which the benefits realized in its current, limited form can contest with a full accounting of its costs.

Part I.B detailed serious shortcomings with the consensus approach to privacy law. There are, in other words, good reasons to doubt that privacy laws today are meaningfully addressing surveillance abuses rife in the information economy.[330] But privacy law falling short of its stated aims is not some costless folly. Part III showed that privacy law's consent-and-control approach confers advantages on the same dominant incumbent firms that the recent wave of legislative action purportedly reins in. As Part IV.A.1 argued, the proper aims of competition law should be restraining concentrated economic power,

mitigating the GDPR's anticompetitive effects); Peukert, *supra* note 221, at 26 ("We find that while the market for third-party web technologies shrank in the period following the GDPR's enactment, Google's position in various web technology markets improved relative to competitors. Increasing concentration and an increasing market share of the dominant firm is most likely not what European legislators had in mind when designing the GDPR. Indeed, the European Commission stressed in 2012 how the pro-competitive effects of the future GDPR would increase the attractiveness of Europe as a location to do business."). Whatever the eventual success of the DMA, its competition mandates are widely understood to raise privacy and security concerns. *See supra* note 210 and accompanying text. So the tension articulated in Part III.B will remain palpable, and domestic policymakers would be wise to observe the GDPR's and DMA's tradeoffs closely.

[330] *See, e.g.*, Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776, 792-815 (2020) (extensively detailing the ways the privacy compliance has been gamified and managerialized — with limited benefits to privacy).

and policymakers and commentators are right to have grave misgivings about ungovernable corporate behemoths and the accumulation of unaccountable authority over the global information ecosystem. Together, these pieces paint an unflattering portrait of the status quo: concern about dominant informational platforms is warranted and precipitated a raft of new privacy laws, but those laws aren't achieving their stated ends — and are instead further entrenching their ostensible targets.

The consent-and-control paradigm's role in the powers of incumbency are significant. Part III.A illustrated that the paramount importance of consent makes compliance easiest for the largest companies, since obtaining consent amounts to a software-creation mandate, and the biggest firms produce software most cost effectively. Part III.B showed how consent affords dominant companies with a novel basis for cutting off rivals' access to their data by citing their legal obligations to protect the users' privacy. And Part III.C suggests that the stronger a consent-based privacy rule is, the more it will hurt smaller firms unable to account for data loss, whereas companies with enormous scale will eventually infer around the lost data.

In other words, while many scholars have rightly condemned the consent-and-control paradigm on efficacy grounds, this Article has revealed another basis for doubting its value — that the need to obtain consent advantages incumbents in multiple ways. A privacy-law regime that eschewed consent-as-a-free-pass would look different from the status quo in many ways, but if there is any hope that privacy law can assist with restraining platform dominance — rather than reinforcing it — it lies in a vision of privacy law beyond the consent-and-control paradigm.

2. Beyond Consent and Control

As the fundamental shortcomings of the prevailing approach have become apparent, scholars have urged policymakers to think outside the box — to envision an information regulatory regime that isn't just "an exercise in managerial box-checking."[331]

[331] Cohen, *supra* note 48.

Salomé Viljoen, for example, has urged a shift from individualized notions of privacy law to a democratic data-governance regime — one that pursues "data production for the public interest, undertaken with strong forms of public accountability, purpose limitations, and confidentiality standards."[332] Julie Cohen has argued that responding to surveillance-based business models' dysfunctions "requires moving beyond reactive conceptions of data protection toward a governance model organized around problems of design, networked flow, and scale, and framed in terms of concrete requirements that must be satisfied by firms collecting, processing, and exchanging personal information."[333] Ari Waldman has pressed policymakers to "start becoming more comfortable with two words that are gaining increasing prominence among scholars and advocates: 'ban it.'"[334] Specifically and as salient here, he argues we "should consider bans on collecting certain types of information" and "bans on certain uses of information."[335]

Not only do these scholarly approaches suggest a regime that goes beyond legitimizing the status quo, a more muscular interpretation of privacy law's means and ends promises to more effectively restrain platform dominance too.

Online behavioral advertising — often referred to as targeted advertising — provides a concrete example of the shift urged here. The European Union concluded that Meta was prohibited from using its terms of service to require users of its platforms to accept personalized advertising.[336] In response, Meta has attempted to offer EU users the choice of accepting targeted advertising or paying a monthly fee, which the European Data Protection Board has also contested.[337] The decisions

[332] Viljoen, *supra* note 48, at 644.

[333] Cohen, *supra* note 48.

[334] Waldman, *supra* note 183, at 239.

[335] *Id.* at 239.

[336] *See* Press Release, Irish Data Prot. Comm'n, Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland (Jan. 4, 2023), dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland [https://perma.cc/RZ2P-4B85]; Sam Schechner, *Meta's Targeted Ad Model Faces Restrictions in Europe*, WALL ST. J. (Dec. 6, 2022), wsj.com/articles/metas-targeted-ad-model-faces-restrictions-in-europe-11670335772.

[337] *See generally Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, EUR. DATA PROT. BD. (Apr. 17, 2024),

are part of a long-running dispute over how to interpret the GDPR's bases for data processing, which means that they ultimately hinge on a question of consent.[338]

An information-governance regime that would both limit the power of dominant informational platforms while also protecting privacy would take the decision one step further — banning targeted advertising outright. A full accounting of the costs, benefits, and impacts of overtly regulating automated attention markets are beyond the scope of this Article.[339] But there should be little doubt that outlawing targeted advertising would seriously impair the profitability of dominant informational platforms and would likely expose them to competitive pressures that are unimaginable in the current environment. A company of Meta's scale would of course start with a significant head start in adapting to a world limited to contextual advertising, but a ban on personalized advertising would nevertheless vitiate much of the competitive moat that Meta has constructed over the past fifteen years.

edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf [https://perma.cc/5KUM-C2UR] (concluding that Meta's proposed "pay or okay" model violates the GDPR's requirement to obtain "freely given" consent).

[338] *See* Natasha Lomas, *Meta's New Year Kicks Off with $410M+ in Fresh EU Privacy Fines*, TECHCRUNCH (Jan. 4, 2023, 7:00 AM PST), techcrunch.com/2023/01/04/facebook-instagram-gdpr-forced-consent-final-decisions/ [https://perma.cc/29HR-X65V].

[339] S*ee also* Peter Ormerod, *Regulating Data Monetization* (unpublished manuscript) (draft on file). *See generally* Daniel Susser, *From Procedural Rights to Political Economy: New Horizons for Regulating Online Privacy*, *in* THE ROUTLEDGE HANDBOOK ON PRIVACY AND SOCIAL MEDIA 8-9 (Sabine Trepte & Philipp Masur eds., 2023) ("[I]f the very harm regulation aims to prevent — surveillance — is the source of Big Tech's profits, then structural change must take a particular form: remaking the industry's dominant business model. If we are serious about privacy in the digital world, technology firms (especially social media companies) will have to find new ways to make money."); Derek E. Bambauer, *Target(ed) Advertising*, 58 UC DAVIS L. REV. __ (forthcoming 2025) (arguing for limited reforms to the targeted-advertising industry); Jeff Gary & Ashkan Soltani, *First Things First: Online Advertising Practices and Their Effects on Platform Speech*, KNIGHT FIRST AMEND. INST. (Aug. 21, 2019), knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech [https://perma.cc/2ZHM-D3N7] (arguing for a ban on targeted advertising); K. Sabeel Rahman & Zephyr Teachout, *From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure*, KNIGHT FIRST AMEND. INST. (Feb. 4, 2020), knightcolumbia.org/content/from-private-bads-to-public-goods-adapting-public-utility-regulation-for-informational-infrastructure [https://perma.cc/QW7R-RGXU] (advocating for a ban on targeted advertising).

It remains true, as noted at the outset of Part III.A, that any regulatory regime may benefit incumbents to some extent, but a data-governance regime concerned with how companies use their own data ameliorates the worst pathologies of all three powers of incumbency. Rendering consent irrelevant obviates the advantages that dominant companies realize in obtaining consent, and limiting how data may be used and monetized will reduce the competitive benefits associated with content fortresses.

Advertising technology industry insiders discuss the recent GDPR decisions in apocalyptic terms,[340] which illustrates the threat posed to the status quo by an information-governance regime that shifts away from red herrings about consenting to third-party sharing and towards a reckoning over first-party use. It would be a mistake, though, to accept their framing at face value. Current law already limits how companies may use data in a rich panoply of ways, and those restrictions have tended to prove enduring and popular. The Fair Credit Reporting Act is this country's oldest consumer privacy law, and it was enacted in response to widespread abuses in the credit-reporting industry in the 1960s. Credit-reporting companies collected any and all available information — from sexual orientation to alcohol-consumption habits — and shared those dossiers with the police, but never the subjects.[341] The Fair Credit Reporting Act stringently regulates how credit-reporting companies may use data, and it cracked down on at least three aspects of the prevailing information ecosystem: limiting what information may permissibly be included in a credit report,[342] imposing an obligation to make the data available to the subject,[343] and limiting to

[340] *See* John Gruber, *European Data Protection Board Goes There, Rules Against Meta's 'Pay or OK' Model*, DARING FIREBALL (Apr. 17, 2024), daringfireball.net/2024/04/edpb_meta_pay_or_ok [https://perma.cc/4RW9-A43G]; Ben Thompson, *Meta's EU Fine; First-Party Versus Third-Party Data, Redux; The EU's First Party Imposition*, STRATECHERY (Jan. 11, 2023), stratechery.com/2023/metas-eu-fine-first-party-versus-third-party-data-redux-the-eus-first-party-imposition/ [https://perma.cc/3G68-9TM9]; Thompson, *supra* note 157.

[341] *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 271 (Cambridge Univ. Press 2016).

[342] *See* 15 U.S.C. § 1681c.

[343] *See* 15 U.S.C. § 1681h.

whom the companies may disclose the information and for what purpose.[344]

A more recent example is the Affordable Care Act. Before it was enacted, health insurers denied coverage based on preexisting conditions and price discriminated based on health history.[345] The law's Guarantee Issue and Community Rating provisions outlawed both — requiring, respectively, that insurers issue a policy to anyone and charge uniform prices irrespective of health condition or history.[346] Though not conventionally understood this way, these provisions are exactly the sort of democratic data-governance regime envisioned here: before the law was enacted, health insurers used personal information to refuse service and price discriminate, and the law prohibited them from monetizing their data in these ways.

Policymakers should internalize lessons from data-use limitations like these and reject industry insiders' contentions that regulators must concern themselves only with third-party data sharing. There are some promising signs that policymakers are starting to move in this direction. The FTC has recently proposed a blanket ban on Meta's ability to monetize youths' data,[347] and seventeen municipalities to date have banned the use of facial recognition.[348]

If data ultimately is the source of platform power, an information-governance regime that checks unaccountable power, promotes competition, *and* protects privacy is one that infuses democratic accountability into the terms under which data is used and monetized.

---

344 *See* 15 U.S.C. §§ 1681b, 1681d, 1681f, 1681g.

345 *See* Giampiero Marra, Rosalba Radice & David Zimmer, *Did the ACA's "Guaranteed Issue" Provision Cause Adverse Selection into Nongroup Insurance? Analysis Using a Copula-Based Hurdle Model*, 30 HEALTH ECON. 1 (July 2, 2021) ("Prior to the Affordable Care Act (ACA), insurance companies could charge higher premiums, or outright deny coverage, to people with preexisting health problems.").

346 *See* 45 C.F.R. §§ 147.104, 147.108, 147.110.

347 Press Release, Fed. Trade Comm'n, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data [https://perma.cc/ZG7N-7EH3].

348 *See* Nathan Sheard &Adam Schwartz, *The Movement to Ban Government Use of Face Recognition*, ELEC. FRONTIER FOUND. (May 5, 2022), https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition [https://perma.cc/R5P8-CNBU].

***

The powers of incumbency pose a difficult quandary for those who wish to hold dominant technology companies accountable. Consent-based privacy laws further entrench the biggest firms without doing much in the way of protecting privacy. But policymakers who seek a competition-based solution are likely to make privacy problems much worse, since increased competition incentivizes new surveillance abuses and competition-maximizing policy responses undermine privacy laws. The solution, therefore, should be focused on our conception of privacy law. This Part has shown that consent-based privacy laws are not just ineffective — a consent-and-control foundation is the source of privacy law's incumbent-advantaging force. To restrain concentrated and unaccountable power over the information ecosystem requires an information-governance regime that speaks explicitly to how firms can monetize data.

CONCLUSION

A small number of technology companies today exercise outsized control over the information economy and thereby the engine of twenty-first-century prosperity. Scholars and policymakers are searching for effective tools to hold them to account, and so far, they've employed well-worn tactics like returning antitrust law to an earlier era and erecting privacy law's fifty-year-old notice-and-choice scaffolding onto the digital economy. Those efforts have fallen short of their aims, and one contributing reason for that failure is a lack of understanding about how these doctrinal silos interact in digital markets.

The prevailing scholarly consensus is that competition and privacy are in a harmonious, correlative relationship — that more competition will produce more privacy. This Article has shown the opposite: that consent-based privacy rules confer three potent advantages on entrenched incumbents, which means that they undermine competition and further enrich the laws' ostensible targets. Armed with a full accounting of privacy law's incumbency problem, policymakers have new clarity about the challenges they face.