Yale Journal of Law & Technology
Volume 28, Symposium Issue

Disciplining Mechanisms: Governing Data Markets with Competition and Regulation

Peter Ormerod[*]

The past decade has witnessed conceptual renewals in both competition law and information privacy law. These regulatory movements—Neo-Brandeis antitrust and structural data governance—share the objective of recalibrating the balance of power between individuals and the massive data-processing firms that now dominate modern life.

Despite their common ends, policy interventions drawn from these schools of thought can work at cross purposes: competitive pressure can induce data exploitation, and privacy rules tend to benefit the largest firms.

This Essay exposes the friction in their relationship and offers guidance on how to mediate their tension. Competition policy alone will prove ineffective at indirectly disciplining most data activities, so policymakers should largely favor the structural data-governance approach to address the information economy's pathologies. But pro-competition policies will nevertheless be essential to reining in firms that are too big to meaningfully regulate and may also prove helpful in solving certain discrete data-processing problems.

Policymakers today have two distinct mechanisms for disciplining firms' data-driven activities. This Essay describes them, exposes their contours, and offers those policymakers guidance on how best to deploy them.

---

[*] Associate Professor of Law, Villanova University Charles Widger School of Law. My thanks to Greg Elinson and Ryan Fore for their feedback on prior versions.

Article Contents

Introduction

Companies today generate hundreds of billions of dollars every year using techniques that largely didn't exist a generation ago: processing vast amounts of data to predict and influence individuals' behavior.[1] While these activities are widespread across the information economy, a small number of enormous firms dominate the most profitable digital markets.[2]

In the decades preceding digitization's runaway success, neoclassical academics, policymakers, and jurists waged a concerted campaign to neuter regulatory approaches that could have been responsive to the companies and business models that now dominate.[3] The Chicago School of antitrust and a neoliberal approach to consumer protection helped ensure that little stood in the way of the novel and profitable data activities—and the firms deploying them—that now pervade modern life.[4]

But now a conceptual renewal is afoot. Since the aftermath of the global financial crisis—particularly in the past decade—academics and policymakers have revisited the assumptions underlying the neoliberal consensus.[5] When it comes to large technology companies, some of these post-neoliberal scholars have sought to remake competition law, while others have focused on more overt forms of regulation.[6]

Despite their shared objectives, these new approaches do not invariably enjoy a harmonious relationship. How and when policymakers employ each tool will have profound implications in the coming generation. This Essay exposes the friction in

---

[1] *See generally* Amanda Parsons & Salomé Viljoen, *Valuing Social Data*, 124 COLUM. L. REV. 993 (2024).

[2] *See, e.g.*, Peter Ormerod, *Privacy Law's Incumbency Problem*, 58 U.C. DAVIS L. REV. 179, 181–82 (2024).

[3] *See, e.g.*, Luke Herrine, *At the Nexus of Antitrust & Consumer Protection*, 2023 UTAH L. REV. 849, 851 (2023).

[4] *Id.*

[5] *See* Luke Herrine, *Unfairness, Reconstructed*, 42 YALE J. REG. 95, 100 (2025).

[6] *See id.* at 99; *see also* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 617–34 (2021).

their relationship and offers some preliminary thoughts about how policymakers can make the most of both.

Part I traces the emergence of these new approaches to competition policy and data governance. Part II outlines the tensions between them: pro-competition interventions can induce deleterious data practices, and data regulations tend to benefit the largest incumbent firms. In light of these realities, Part III posits how policymakers should best employ them.

Policymakers today are armed with two distinct mechanisms for disciplining firms' data-driven activities. This Essay describes them, exposes their contours, and offers those policymakers guidance on how to make use of them.

I. Two Regulatory Tools

Over the past generation, a small number of technology companies have accreted greater and greater control over modern life. Meanwhile, two distinct regulatory approaches meant to guard against that sort of capture—competition law and consumer-protection law—stood by the wayside. Only in the past decade have scholars and policymakers begun mounting a pair of counter-movements to Silicon Valley's hegemony. This Part sketches the rise of these renewed regulatory efforts.

A. Neo-Brandeis Antitrust

The neoclassical Chicago School posits that antitrust law's sole concerns are high output and low prices.[7] This consumer-welfare standard severely constrains antitrust enforcement and has dominated antitrust law for over fifty years.[8]

It is little surprise, then, that antitrust law missed the rise of large technology companies.[9] The paradigmatic digital business model consists of giving away products at no charge

---

[7] *See* Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 933 (1979).

[8] *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); TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 108 (2017).

[9] *See* Ormerod, *supra* note 2, 198–200.

other than the data collected from users.[10] The businesses that collect the data in turn use it in a variety of monetization strategies—most prominently and lucratively, for targeted advertising.[11] This data-for-access bargain is thus an ideal fit for escaping neoclassical antitrust scrutiny: because the businesses do not charge the users a price, there are no supra-competitive prices to police.[12] The consumer-welfare standard, in other words, regards the rise of informational platforms like Google's and Meta's as pure upside; users pay no money to gain access to a wide array of digital services.

It has only been in the past decade that scholars and policymakers have coalesced around an account of competition law that challenges this conventional wisdom. While this countermovement is no monolith and has several different facets and labels, I'll refer to it here as the Neo-Brandeis movement.[13]

---

[10] *See* JULIE E. COHEN, BETWEEN TRUTH & POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM 42–43 (2019); Amy Kapczynski, *The Law of Information Capitalism*, 129 YALE L.J. 1460, 1507 (2020).

[11] *See* Peter Ormerod, *Regulating Data Monetization*, 13 TEX. A&M L. REV. __, 22–26 (forthcoming 2026).

[12] *See* Ormerod, *supra* note 2, at 199.

[13] *See, e.g.*, Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. EUR. COMPETITION L. & PRAC. 131 (2018) ("New Brandeis"); Lina M. Khan, *The End of Antitrust History Revisited*, 133 HARV. L. REV. 1655, 1665–71 (2020) (reviewing WU, *supra* note 8) ("Neo-Brandeis"); Matthew Sipe, *Covering Prying Eyes with an Invisible Hand: Privacy, Antitrust, and the New Brandeis Movement*, 36 HARV. J. L. & TECH. 359 (2023) (same); Joshua D. Wright, Elyse Dorsey, Jan Rybnicek & Jonathan Klick, *Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust*, 57 ARIZ. ST. L. J. 293 (2019) ("Hipster Antitrust"); Erika M. Douglas, *The New Antitrust/Data Privacy Interfac*e, 130 YALE L.J. F. 647, 652 (2021) ("Integrationist"); Nolan McCarty & Sepher Shahshahani, *Testing Political Antitrust*, 98 N.Y.U. L. REV. 1169 (2023) ("Political Antitrust"); Daniel Susser, *From Procedural Rights to Political Economy: New Horizons for Regulating Online Privacy*, at *8–9, *in* THE ROUTLEDGE HANDBOOK OF PRIVACY AND SOCIAL MEDIA (Sabine Trepte & Philipp Masur eds., 2023) ("New Antitrust"); Marshall Steinbaum & Maurice E. Stucke, *The Effective Competition Standard: A New Standard for Antitrust*, 86 U. CHI. L. REV. 595 (2019) ("Effective Competition"); Nathan Tankus & Luke Herrine, *Competition Law as Collective Bargaining Law*, *in* THE CAMBRIDGE HANDBOOK OF LABOR IN COMPETITION LAW 72 (2022) ("Neochartalist microeconomics"; "Modern Monetary Theory").

The publication of former chair of the Federal Trade Commission Lina Khan's student note, *Amazon's Antitrust Paradox*, marked an important turning point.[14] Follow-on work by Khan and other policymakers like former assistant attorney general for the Department of Justice's antitrust division Jonathan Kanter and National Economic Council special assistant Tim Wu further refined the principles of the Neo-Brandeis movement.[15]

As contrasted against the Chicago School's consumer-welfare standard, Neo-Brandeisians start with the premise that supra-competitive prices do not capture the full breadth of harms and risks posed by large concentrations of economic power.[16] Competition law should thus concern itself with a broader set of social and political considerations by focusing on the structures and process of competition rather than outcomes.[17] In an elucidating synthesis, Luke Herrine explains that as "an alternative to consumer welfare, Neo-Brandeisians argue for a form of antitrust that seeks to disperse power, distribute opportunity, promote fair treatment, and channel competition toward labor-saving and quality-improving (rather than output-maximizing) innovation."[18] Sanjukta Paul has highlighted the "moral economy" foundations of antitrust law by showing how the Sherman Antitrust Act was enacted against a rich restraint-of-trade common law.[19] This fuller account suggests that antitrust law should do more than just police prices: it should contain domination, promote democratic coordination, and set the rules of fair competition.[20]

---

[14] *See* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017).
[15] *See* Khan, *New Brandeis*, *supra* note 13; WU, *supra* note 8; Khan, *The End of Antitrust History Revisited*, supra note 13; Jonathan Kanter, *Remarks for the Fordham Competition Law Institute's 51st Annual Conference on International Antitrust Law and Policy* (Sept. 12, 2024), http://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-delivers-remarks-fordham-competition-law-0 [https://perma.cc/EMA9-CD2C].
[16] *See* Herrine, *supra* note 3, at 867–70; Sipe, *supra* note 13, at 388.
[17] *See id.*; Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, *supra* note 13, at 132.
[18] Herrine, *supra* note 3, at 869.
[19] *See* Sanjukta Paul, *Recovering the Moral Economy Foundations of the Sherman Act*, 131 YALE L.J. 175, 190–98 (2021).
[20] *Id.* at 179, 247–54.

This wider aperture means that the Neo-Brandeisians mark a sharp break from the Chicago School when it comes to data-intensive businesses. A decreased emphasis on price—and an increased emphasis on product quality—renders targeted-advertising-based informational platforms legible to competition law. As Kanter puts it, this new approach to antitrust enforcement "tak[es] a broad view and an aggressive posture in identifying harms to the competitive process as a whole, including harms to privacy, innovation, and other important equities that go beyond price."[21]

Casting privacy as a site of non-price quality competition has two related implications. First, competitive markets should produce greater privacy protections. Second, policymakers should overtly consider the privacy implications of their enforcement actions—or inaction.[22] Meta provides an apt illustration of both. Dina Srinivasan has demonstrated the former in how Facebook initially competed "in a contested market [using] superior representations of protecting consumer privacy, including the specific promise not to track and monitor consumers' digital footprints."[23] The app's surveillance-based infrastructure became inescapable only after it came to dominate the social-networking space.[24] The perils of policymakers' failure to consider the privacy

---

[21] Oversight of Federal Enforcement of the Antitrust Laws: Hearing Before the S. Judiciary Comm. Hearing on Competition Pol'y, Antitrust, and Consumer Rts., 118th Cong. (2022) (statement of Jonathan Kanter, U.S. Assistant Att'y Gen.), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-testifies-senate-judiciary [https://perma.cc/78MX-ZM2B]; *see also* Markan Delrahim, *Assistant Attorney General, Remarks for the Antitrust New Frontiers Conference*, DEP'T OF JUSTICE (June 11, 2019), https://www.justice.gov/opa/speech/assistant-attorneygeneral-makan-delrahim-delivers-remarks-antitrust-new-frontiers [https://perma.cc/3XJG-PEDR] ("[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.").

[22] *See* Ormerod, *supra* note 2, at 202–03.

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

[24] *See id.* at 44–45.

implications of consolidation in the tech sector is evidenced by the deterioration of WhatsApp's data practices following its acquisition by Meta.[25]

Led by Khan, Kanter, and Wu, the Biden administration's competition policies pursued these principles. The FTC's 2022 Policy Statement reflects and codifies this focus on broader competitive harm, including product quality.[26] Chair Khan brought antitrust cases against Meta and Amazon that identified competitive harms beyond prices and output.[27] And under Kanter, the DOJ pursued multiple monopolization cases against Google that overtly incorporate Neo-Brandeisians' broader conception of competitive harms.[28]

B. Structural Data Governance

In parallel to the Neo-Brandeis antitrust movement, there has also been an effort to reimagine more direct regulation of firms' data activities.

Information privacy law in the United States has traditionally been regarded as a specific type of consumer protection law.[29] The principal source of generally applicable privacy rules has long been the FTC's authority over unfair and deceptive trade practices.[30] The neoliberal ideal of consumer sovereignty—that is, "a hypothetical condition in which consumers incidentally discipline the conduct of firms simply

---

[25] *See* Maurice E. Stucke, *The Relationship Between Privacy and Antitrust*, 97 NOTRE DAME L. REV. REFLECTIONS 400, 402–03 (2021).

[26] *See* Fed. Trade Comm'n, *Policy Statement Regarding the Scope of Unfair Methods of Competition under § 5 of the Federal Trade Commission Act* 9–10 (Nov. 10, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/p221202sec5enforcementpolicystatement_002.pdf [https://perma.cc/KHQ7-WX3A].

[27] *See* FTC v. Meta Platforms Inc., 654 F. Supp. 3d 892, 921 (N.D. Cal. 2023); Complaint, FTC v. Amazon, Inc., 2:23-cv-01495-jhc (W.D. Wash. Nov. 2, 2023).

[28] *See* Complaint, United States v. Google LLC, No. 23-cv-00108 (E.D. Va. Jan. 24, 2023) (bringing suit for digital advertising practices); United States v. Google LLC, 2024 WL 3647498, Nos. 20-cv-3010 (APM), 20-cv-3715 (APM) (D.D.C. Aug. 5, 2024) (bringing suit for default search deals).

29. *See* Ormerod, *supra* note 2, at 184–85 n.21; Ormerod, *supra* note 11, at 7.

[30] *See* Ormerod, *supra* note 11, at 7 (citing Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014)).

by shopping"[31]—has pervasively informed the FTC's approach to consumer protection for most of privacy law's history.[32] So long as "consumers know what they want and know what is available and firms are forced to compete for consumers' business, consumer choice on the free market will produce the mix of good and services (and, indeed, social conditions more broadly) that best furthers consumers' interests."[33]

These assumptions—that given information ("notice"), consumers will make wise decisions ("choice")—are encoded into domestic privacy law from top to bottom.[34] Not only do older sectoral privacy laws like the Fair Credit Reporting Act employ this notice-and-choice paradigm, but so do recent omnibus consumer privacy laws like the California Consumer Privacy Act.[35]

Privacy scholars in recent years have sharply criticized the notice-and-choice paradigm.[36] They've observed that "even well-informed and rational individuals cannot appropriately self-manage their privacy" because it is "impossible for people to weigh the costs and benefits of revealing information or permitting its use."[37] The ease with which firms mislead the public about the reality of their data practices means that it is all too easy for companies to rely on vague, pro-privacy representations.[38] Executives at the low-cost television manufacturer Vizio prove the point when—despite paying millions of dollars in fines for collecting customers' data without consent—they claim that "Vizio has been pioneering privacy and active viewing data disclosures for the last several

---

[31] Herrine, *supra* note 5, at 99.
[32] *See id.* at 99–100; *see also* Ormerod, *supra* note 2, at 198–99.
[33] Herrine, *supra* note 5, at 99–100.
[34] *See* Viljoen, *supra* note 6, at 593–94.
[35] *See id.*; Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS ONLINE 19, 34, 38 (2021).
[36] *See* Ormerod, *supra* note 11, at 11–23.
[37] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013).
[38] *See, e.g.*, ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER xi-xv (2021). The book's dust jacket memorably recites the substance-less incantation "Your Privacy Is Important to Us" innumerable times.

years, and we actually lead the industry in those disclosures."[39] It's also shockingly easy for data collectors to dupe users into revealing as much information as possible; they need only misleadingly signal benevolent motives to induce people to trust them and thereby disclose more information.[40]

Even companies with seemingly strong privacy bona fides are guilty of obscuring the truth from their users. DuckDuckGo, the privacy-protecting alternative to Google search, is an oft-invoked example of a company that distinguishes itself from competitors based on its higher-quality data practices.[41] But even this poster child of privacy-as-quality has been caught giving Microsoft privileged access to its users' data.[42] Similarly, companies that stridently promise to resist the data-monetization imperative often reverse course when their venture investors demand it.[43] The simple reality of Silicon

---

[39] Nilay Patel, *Taking the Smarts Out of Smart TVs Would Make Them More Expensive*, THE VERGE (Jan. 7, 2019, 4:46 PM), http://www.theverge.com/2019/1/7/18172397/airplay-2-homekit-vizio-tv-bill-baxter-interview-vergecast-ces-2019 [https://perma.cc/A2CB-2ZBN] (quoting Vizio's CTO); *see also* 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), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11million [https://perma.cc/3SBJ-CMRH].

[40] *See, e.g.*, 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*, 21 J. EMPIRICAL LEGAL STUD. 577 (2024).

[41] *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).

[42] *See* Andy Greenberg, *Security News This Week: DuckDuckGo Isn't as Private as You Think*, WIRED (May 28, 2022, 9:00 AM), http://www.wired.com/story/duckduckgo-microsoft-twitter-ft-bush-assassinationwhatsapp/ [https://perma.cc/CTF5-C2FH].

[43] *See, e.g.*, Casey Newton, *The Ad Model is Coming to AI*, PLATFORMER (Apr. 1, 2024), http://www.platformer.news/perplexity-ai-ads-privacy-risks [https://perma.cc/X852-7WZM] ("[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.").

Valley today is that it has a singular focus on the short-term maximization of companies' self-defined "key performance indicators."[44]

There is no back-end accountability for these falsities, either. Constrained enforcement authority ensures that a tiny number of regulators bring a small sliver of potential enforcement actions against only the most egregious and visible offenders.[45]

In short, data-governance scholars have convincingly shown that relying on individuals to make wise decisions about their information is not only a doomed, futile endeavor, but also that empowering consumers ought not be privacy law's highest ideal since it misapprehends the actual, collectivist stakes of datafication.[46] In its stead, they've offered a vision of data governance that operates at a structural—rather than individualized—level.[47]

For example, Frank Pasquale has advocated in favor of an algorithmic licensing regime.[48] "A licensure regime for data and the AI it powers," he explains, "would enable citizens to democratically shape data's scope and proper use, rather than resigning ourselves to being increasingly influenced and shaped

---

[44] *See* Zvi Mowshowitz, *GPT-4o Is An Absurd Sycophant*, DON'T WORRY ABOUT THE VASE (Apr. 28, 2025), https://thezvi.substack.com/p/gpt-4o-is-an-absurd-sycophant [https://perma.cc/F5AE-6MB9] ("My observation of algorithms in other contexts (e.g. YouTube, TikTok, Netflix) is that they tend to be myopic and greedy far beyond what maximizes shareholder value. It is not only that the companies will sell you out, it's that they will sell you out for short term KPIs.").

[45] *See, e.g.*, Peter Ormerod, *Privacy Qui Tam*, 98 NOTRE DAME L. REV. 267, 283–84 (2022) (quoting Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS: TECHTANK (Aug. 8, 2019) http://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/LE8Z-UW9Q]; Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST., at 17 (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/86N2-Q9LA].

[46] *See id.* at 11–16 (ineffective means); *id.* at 16–22 (dubious ends).

[47] *See* Susser, *supra* note 13, at *3–6.

[48] Frank Pasquale, *Licensure as Data Governance*, KNIGHT FIRST AMEND. INST. (Sept. 28, 2021), https://knightcolumbia.org/content/licensure-as-data-governance.

by forces beyond our control."[49] K. Sabeel Rahman and Zephyr Teachout have urged policymakers to draw on public utility regulation to govern large informational platforms, which could impose "mandates for fair treatment, common carriage, and nondiscrimination as well as limits on extractive pricing and constraints on utility business models."[50] This approach—which some have begun calling networks, platforms, and utilities (NPU) law—explicitly seeks to tie online marketplaces, web search, social media, and AI to historical approaches to regulating communications, transportation, and energy.[51] Many others have called for outlawing the surveillance-based advertising model altogether.[52] Neil Richards and Woody Hartzog have proposed imposing loyalty obligations on data collectors,[53] and Ari Waldman has called for banning some data-collection and data-use activities.[54]

In recent work, I have offered a framework that ties several of these strands together. The proper target of structural data governance, I argue, is how firms monetize data through individualized differentiation—the process of offering customized, personalized, or otherwise distinct products,

---

[49] *Id.* at 4.

[50] *See* 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), at 6, https://knightcolumbia.org/content/from-private-bads-to-public-goods-adapting-public-utility-regulation-for-informational-infrastructure [https://perma.cc/4EDV-2ARB].

[51] *See generally* MORGAN RICKS, GANESH SITARAMAN, SHELLEY WELTON, AND LEV MENAND, NETWORKS, PLATFORMS, AND UTILITIES: LAW AND POLICY (2022) (marrying the former and latter in one casebook).

[52] *See, e.g.*, Jeff Gary & Ashkan Soltani, *First Things First: Online Advertising Practices and Their Effects on Platform Speech*, KNIGHT FIRST AMEND. INST. (Aug. 21, 2019), https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech [https://perma.cc/T4PG-F9M5]; Jack Balkin, *To Reform Social Media, Reform Information Capitalism*, *in* SOCIAL MEDIA, FREEDOM OF SPEECH AND THE FUTURE OF OUR DEMOCRACY (Lee Bollinger & Geoffrey R. Stone eds., 2022); Susser, *supra* note 13, at *8–9.

[53] Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021).

[54] ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 239 (2021).

services, experiences, and prices to customers, users, employees, and other counterparties. [55] Collecting and analyzing massive amounts of information about human activity enables companies to predict and modulate behaviors at scale, producing a differentiation premium: the difference between what a data processor charges for an undifferentiated offering and one that reflects the processor's ability to apprehend, predict, and modulate a counterparty's behavior to extract maximum surplus.[56] Considering this broader family of related informational activities takes data governance beyond the traditional spheres of consumer-protection-based information privacy law, extending it to risk-profiling in insurance; first-degree price, wage, and rent discrimination; algorithmic personalization; and more.[57]

* * *

In the past decade, the prevailing accounts of competition law and privacy law have come under enormous pressure from a new generation of scholars and policymakers. These new approaches contest foundational premises of each field: that prices capture the full breadth of competitive harm and that informational rights are the best mechanism for governing data. Despite—or perhaps because of—their shared desire to address the potent concentration of power in a small number

---

[55] *See* Ormerod, *supra* note 11, at 23–26.

[56] *Id.* at 24 ("To take one concrete example, the differentiation premium is the difference between the price a platform charges for a targeted advertisement versus the price charged for an untargeted one. To take another, the differentiation premium is the difference between what a life insurance company charges a healthy 40-year-old and another with cancer."); *see also* Parsons & Viljoen, *supra* note 1, at 1038; Cohen, *supra* note 10, at 95.

[57] *See* Ormerod, *supra* note 11, at 26–34; *see also* Salomé Viljoen, *The Broader Lessons of Privacy Law*, 104 B.U. L. REV. 1131, 1148–49 (2024) ("[M]uch of the recent development in 'privacy law' presents a body of legal theoretical work that apprehends the growing entanglement of privacy—and its historical preoccupation with how information links people, constitutes, empowers and imperils them—with an ever-growing list of other social and legal concerns. . . . Relegating these insights to the category of 'privacy law' alone—even an expansive category—undersells their general legal theoretical value for understanding legal relations in an informational society. In other words, the methods or approaches that have grown from decades of privacy analysis can describe, illuminate, or resolve many *other* kinds of legal issues.").

of large technology firms, scholars have paid relatively scant attention to the question of how these regulatory tools interact with one another. The next Part takes up that task.

II. Competition & Data Governance at Odds

For most of their history, competition and privacy law have been considered isolated doctrinal silos.[58] In recent years, though, scholars have increasingly recognized that their interaction is governed by a set of complex and countervailing dynamics. This Part sheds light on those dynamics.

A. Competition's Effects on Datafication

Neo-Brandeis antitrust suggests that competition and privacy are in a happy, correlative relationship: since privacy protections are a non-price quality parameter that firms compete over, competitive markets should produce a rich array of privacy protections.[59] Firms are only able to escape with cut-rate data practices, the thinking goes, because our digital markets are mostly monopolistic or oligopolistic.

I have explained elsewhere I don't think that's quite right.[60] While I will grant that competition can produce higher-quality data practices in some circumstances, the theory misses a far more prevalent dynamic: firms in fiercely competitive markets will grasp for any edge over their peers, making ever-more invasive data exploitation irresistible.

The television-manufacturing industry provides an apt illustration. Mid- and high-end manufacturers like LG, Samsung, and Sony have traditionally made relatively modest margins on the sale of each set.[61] Vizio and Roku, two low-cost

---

[58] *See* Ormerod, *supra* note 2, at 184–85.
[59] *See id.* at 255.
[60] *See generally id.* at 207–48.
[61] *See* Eric A. Taub, *If There's a High-Definition TV in Your Future, Wait Till After the Holidays*, N.Y. TIMES (Aug. 25, 2007), https://www.nytimes.com/2007/08/25/business/yourmoney/25TELE.html [https://perma.cc/D4RE-898Z]; Nilay Patel, *Taking the Smarts Out of Smart TVs Would Make Them More Expensive*, THE VERGE (Jan. 7, 2019, 4:46 PM), https://www.theverge.com/2019/1/7/18172397/airplay-2-homekit-vizio-tv-bill-baxter-interview-vergecast-ces-2019 [https://perma.cc/7S8B-Q8HS] (quoting Vizio's CTO: "This is a cutthroat industry. It's a 6-percent margin industry, right? I mean, you know it's pretty ruthless").

alternatives, pioneered an alternative business model: selling sets at or below cost and making all of their profit through surveilling customers.[62] This might initially seem to validate Neo-Brandeisian theory: this is a competitive market with a diversity of prices that allow consumers to choose between low-cost-low-privacy and high-cost-high-privacy alternatives.

But over time, the supposedly high-privacy offerings have increasingly viewed the low-privacy alternatives' datafication revenues with envy.[63] LG now brags about sharing its customer data to create "the largest [automatic content recognition] data footprint in the industry."[64] Samsung is building out its sets' surveillance capabilities and crowing about its partnership with Experian, the data broker and financial surveillance leviathan.[65] And an outlandish Sony patent—which would require a television viewer to orally exclaim a brand's name to cease an advertisement—suggests the company is keenly interested in finding new ways to monetize its customers.[66] Ultimately, since customers do not seem to understand these surveillance activities but *do* seem to like cheap TVs, there is little reason for even the higher-end options to eschew ever more data collection and processing. Instead of diverse privacy

---

[62] *See* Daniel Frankel, *Your TV set has become a digital billboard. And it's only getting worse.*, ARS TECHNICA (Aug. 19, 2024), https://www.arstechnica.com/gadgets/2024/08/tv-industrys-ads-tracking-obsession-is-turning-your-living-room-into-a-store/ [https://perma.cc/933C-822L].

[63] *See id.* ("In recent years, we've seen companies like LG and Samsung increase their TVs' ad capabilities as advertisers become more eager to access tracking data from TVs.").

[64] *Id.* Automatic content recognition (ACR) is "a kind of ad surveillance technology that collects data on everything you view and sends it to a proprietary database to identify what you're watching and serve you highly targeted ads." Mohamed Al Elew & Gabriel Hongsdusit, *Your Smart TV Knows What You're Watching*, THE MARKUP (Dec. 12, 2023), https://www.themarkup.org/privacy/2023/12/12/your-smart-tv-knows-what-youre-watching [https://perma.cc/ET5T-RW2W]. "ACR identifies what's displayed on your television, including content served through a cable TV box, streaming service, or game console, by continuously grabbing screenshots and comparing them to a massive database of media and advertisements. Think of it as a Shazam-like service constantly running in the background while your TV is on." *Id.*

[65] *See* Frankel, *supra* note 62.

[66] *Id.*

offerings, competition has produced a deleterious race to the bottom.

A growing chorus has recognized these dynamics. Julie Cohen, for instance, has explained that "antitrust-based approaches do not align well with surveillance abuses. . . . [a]nd antitrust interventions designed to extend data flows" for pro-competitive purposes "will only make privacy problems worse if they are not paired with other, privacy-focused interventions."[67] Daniel Susser wryly notes that "it is not obvious why competition amongst surveillance firms should lead to less surveillance overall."[68] NPU law acknowledges that—at least when it comes to actors that meet expansive definitions of a network, a platform, or a utility—competition policy will likely be inadequate.[69] Matthew Sipe has argued that "data privacy is likely not better served by a multiplicity of small, independent firms."[70] Maurice Stucke contends that "more competition will not necessarily improve privacy, especially when the competition itself is toxic."[71] And Jeff Vagle has observed that "it is difficult to see how increased

---

[67] Cohen, *supra* note 45, at 11.

[68] Susser, *supra* note 13, at 9.

[69] *See, e.g.*, Morgan Ricks, Ganesh Sitaraman, Shelley Welton, and Lev Menand, *Symposium Introduction: Networks, Platforms, and Utilities: Law and Policy*, LPE PROJECT BLOG (Feb. 13, 2023), https://www.lpeproject.org/blog/networks-platforms-and-utilities-law-and-policy/ [https://perma.cc/V4QG-LU6E] ("But whereas antitrust law seeks to safeguard the competitive process, NPU law's domain consists primarily of areas 'in which active regulation has been found necessary to compensate for the inability of competition to provide adequate regulation.'" (quoting F.C.C. v. RCA Communications, 346 U.S. 86 (1953))); K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234, 237 (2018) ("The sheer expense of building these roadways or laying telephone cable suggests a role for public investment and provision, since competition is unlikely on its own to provide adequate alternatives."); *see also* Ricks et al., *supra* note 51, at 7 (defining "networks" as "systems, often characterized by 'links' and 'nodes' that connect users to each other or to different places"; defining "platforms" as "centralized spaces . . . designed to facilitate particular economic or social activities"; and defining "utilities" as "provid[ing] essential, general-purpose services to their users on a more or less continuous basis.").

[70] Sipe, *supra* note 13, at 389.

[71] Maurice E. Stucke, *The Relationship Between Privacy and Antitrust*, 97 NOTRE DAME L. REV. REFLECTION 400, 410 (2021).

competition will necessarily lead to increased protections for information privacy."[72]

What explains the tension between them? In my view, the answer lies within the notice-and-choice skepticism outlined above: firms' data practices are too easily obscured, the harms of surveillance too abstract, and disclosure too easily manipulated for individual decision-making to meaningfully influence firms' data activities.[73] Competition law relies on consumers' shopping preferences to indirectly discipline firms' data practices, but that is at odds with the Neo-Brandeisians' larger project of moving consumer protection beyond mere consumer sovereignty.[74] To assume policymakers can rely on firms competing over privacy-as-quality is also to assume that individuals will make rational, informed decisions about firms' data practices. And yet privacy scholars have long cast doubt on that exact premise.

B. Data Governance's Effects on Competition

It is not only that pro-competitive policies may induce further data exploitation, though. The converse is also true: more overt policy interventions tend to benefit and further entrench the largest companies.

Some have argued that firms use privacy as a pretextual justification for engaging in anti-competitive conduct.[75] I think it goes considerably further than that. In past work, I've argued that the new, state-level consumer privacy laws confer three distinct powers of incumbency on entrenched firms. First, large firms have a comparatively easier time building privacy-law compliance regimes.[76] All compliance regimes exhibit

---

[72] Jeffrey L. Vagle, *Privacy's Commodification and the Limits of Antitrust*, 77 ARK. L. REV. 51, 116 (2024).
[73] *See* Ormerod, *supra* note 2, at 194–96; Ormerod, *supra* note 11, at 11–12.
[74] *See supra* notes 5–33 and accompanying text.
[75] *See* Douglas, *supra* note 13, at 662–67; Erica M. Douglas, *Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis*, 97 NOTRE DAME L. REV. REFLECTION 430, 466–70 (2022); 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, 67–68 (2021); Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 101, 122–39 (2022).
[76] Ormerod, *supra* note 2, at 207–13.

economies of scale, but consumer privacy laws are particularly susceptible because they largely operate as software-creation mandates.[77] Software's high cost of development and low cost of distribution allow established firms to absorb these compliance costs because they amortize their development costs over massive user bases.[78] Second, data restrictions deprive insurgents of a potent resource for challenging a dominant incumbent while simultaneously affording companies with a novel basis for exercising property-like control over the data they collect.[79] And third, scale enables the biggest companies to infer around data losses in a way that is unavailable to their sub-scale competitors.[80] Private-sector privacy initiatives like Apple's App Tracking Transparency have illustrated that dynamic by benefitting companies with the most data, like Meta and Google, and harming their smaller competitors like Snap and Pinterest.[81]

My past work ultimately laid the blame for these effects at the feet of the notice-and-choice regime. I argued that (1) firms realize particularly large economies of scale in their compliance with privacy laws when all they must do is obtain consent; (2) firms' ability to gamify adhesion terms—the environment where consent is obtained—supplies them with a potent opportunity to cut off rivals' access to their data; and (3) a consent mechanism gives large firms just enough data to fuel their probabilistic engines while mortally wounding their smaller competitors.[82]

But this is an incomplete account of the incumbency-benefiting effects of data restrictions.[83] Complying with laws

---

[77] *See id.* at 212–13.
[78] *See id.*
[79] *Id.* at 213–26.
[80] *Id.* at 226–39.
[81] *See id.* at 227–37.
[82] *See id.* at 249–50.
[83] I acknowledge here that I'm oversimplifying by conflating "privacy law" and "data governance" with "data restrictions." The recent crop of notice-and-choice consumer privacy laws include data portability rights, which empower users to download and take their data elsewhere—thereby establishing a new data flow, rather than exclusively restricting them. *Cf.* Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORTIA): Assessing Competition, Privacy, Security, and Other*

that eschew consent-as-a-free-pass will still be easiest for the largest firms as long as they continue mandating additional software. Battening down the hatches and restricting data flows in the name of privacy—even without a consent inoculation—will still hamper small firms that need incumbents' data to compete. And large firms' probabilistic engines will remain orders more effective than their smaller rivals even in the absences of any consent-derived data. In other words, there are good reasons to think that the emergent approach to structural data governance will—at least in isolation—also tend to benefit the established players.

Why does privacy law—and data governance more generally—uniquely advantage dominant incumbents? In my view, the dynamic that drives this phenomenon is also the dynamic that drives high levels of concentration in digital markets more generally. Network effects and high fixed costs associated with software development—as others have

---

Considerations, 6 GEO. L. TECH. REV. 57, 57–58 (2022) (acknowledging a tension between data portability and data privacy). The objection is even stronger with regard to structural data governance, which takes as a given that data is an agnostic instrument of power that could—and should!—be put to benevolent, rather than pernicious, ends. *See, e.g.*, Viljoen, *supra* note 6, at 644–50; Daniel Susser, *Data and the Good?*, 20 SURVEILLANCE & SOC'Y 297, 297 (2022); Elettra Bietti, *Data Is Infrastructure*, 26 THEORETICAL INQUIRIES L. 55 (2025). I nevertheless maintain that even structural data governance is, on balance, mostly concerned with restricting whether and how powerful entities like dominant market actors collect and use information, *see, e.g.*, Ormerod, *supra* note 11, at 34–45 (proposing a suite of such restrictions), and data-governance scholars have long recognized the risks associated with surveillance infrastructures that enable the manipulation and modulation of human behavior. *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1917 (2013) ("Modulation is . . . a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories."); BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 2 (2018) ("As we collectively race down the path toward smart techno-social systems that efficiently govern more and more of our lives, we risk . . . becoming increasingly predictable, and worse, programmable, like mere cogs in a machine."). I'll leave for another day the looming debate about whether and when structural data governance reform proposals run counter to at least some definitions of privacy.

recognized—certainly play a role. But I think there is something unique about data-driven markets in particular. Data behaves like a self-perpetuating flywheel: the more you have of it, the more effectively you can monetize it.[84] Business models that exploit data to generate profit at scale thus invariably produce fat tails. Data-governance interventions that restrict data flows will, on balance, benefit the firms that already have a formidable lead in the data-exploitation race.

* * *

The conceptual renewals occurring within antitrust law and privacy law are disrupting the existing consensus in an effort to rein in Silicon Valley's outsized influence over modern life. But less understood is the complex interplay between policies that promote competition to indirectly influence firms' activities and policies that directly prohibit certain data practices. Given the complexities of that interaction, how should policymakers strike a balance between competition and data-governance policies? The next Part offers an answer.

III. Employing Both Competition & Data Governance

Policymakers should not be lured into thinking that competition and data-governance policies are necessarily mutually beneficial. As the previous Part showed, competition can cultivate undesirable data practices, and data governance can benefit incumbents. To effectively recalibrate the balance of power between companies and individuals, policymakers will need to selectively draw from both toolsets.

Start with data governance. If notice-and-choice skepticism is sound, then most data activities cannot be meaningfully disciplined indirectly by additional competitive pressure. To hope that firms competing over product quality will produce high-quality digital offerings is to ignore the growing consensus that the notice-and-choice approach to data governance is a futile and misdirected affair.

---

[84] *See* Ormerod, *supra* note 2, at 226–39; *see also* ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 229–30 (2018); Tejas N. Narechania, *Machine Learning as Natural Monopoly*, 107 IOWA L. REV. 1543, 1584–85 (2022).

Regulatory efforts should thus principally focus on speaking directly to distinguishing permissible and impermissible data-processing practices, with a focus on the practices companies use to transform data into money. Some suggestions I've developed in greater detail elsewhere include banning targeted advertising, imposing tight restrictions on data brokers' surveillance trade, adopting an algorithmic licensing regime, reimagining data-purpose limitations, and levying new taxes on first-party personalization.[85]

Other scholars have similarly cast doubt on competition's ability to discipline data-driven markets. NPU law, for instance, draws attention to the companies that control the bottlenecked intermediation points that enable modern life.[86] While NPU law incisively highlights some of the most egregious examples of data processors weaponizing privileged positions to effect social control and appropriate surplus,[87] those activities—predicting and modulating behavior on an individualized basis at scale—are worthy of strict oversight irrespective of whether the data processor fits the NPU mold.[88]

---

85. *See* Ormerod, *supra* note 11, at 34–45.

86. *Cf.* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM 42 (2019) ("[P]latforms represent both horizontal and vertical strategies of extracting the surplus value of user data. Because that project requires large numbers of users generating large amounts of data, the platform provider's goal is to become and remain the indispensable point of intermediation for parties in its target market.").

87. *See, e.g.*, Brett M. Frischmann, *On the Infrastructural Nature of NPUs*, Notice & Comment Blog, YALE J. REG. (Jan. 18, 2023), https://www.yalejreg.com/nc/symposium-networks-platforms-utilities-02/ [https://perma.cc/Z6AE-HEZP] ("Beyond concerns about competition and innovation incentives, network neutrality resists (seductive promises of) intelligent optimization by infrastructure owners. . . . When a Broadband Internet Access Service ("BIAS") provider knows who is doing what online, the BIAS provider gains power that can be exercised in various ways, such as price discrimination or prioritization. At its core, network neutrality regulation aims to constrain intelligence-enabled social control by infrastructure owners so that users retain their freedom in an under-determined techno-social environment.").

88. *See generally* Ormerod, *supra* note 11. To put a finer point on it, NPU law can obscure the reality that the NPU toolkit can be appropriated by its own subjects "to entrench their dominance over rivals, and to stand in the way of progress . . . ." Amy Kapczynski, *The Political Economy of NPU Law*, Notice & Comment Blog, YALE J. REG. (Jan. 26, 2023),

To be clear, policymakers absolutely should train their focus on the gatekeepers that exercise enormous discretion over our digital infrastructure.[89] While the European Union's Digital Markets Act is a promising step in this direction, it has also revealed a first proper province of reinvigorated antitrust: that we're going to need smaller companies if we want them to actually comply with the structural data-governance policies outlined above.[90]

The size of technology companies today means that they have little reason to meaningfully follow privacy law and consumer-protection law more generally. Because these companies generate enormous profits from exploiting data and because privacy law today is so weak and ineffective, firms have a strong imperative to placate regulators by paying penalties and then resuming business as usual.[91] In other words, violating most of today's data-governance rules is little more than a necessary cost of doing business. In concrete terms, FTC's record-shattering 2019 settlement with Facebook—where the company paid a $5 billion penalty—amounted to only a month

---

https://www.yalejreg.com/nc/symposium-networks-platforms-utilities-09/ [https://perma.cc/NCA6-PTUE]; *see also* Josh Macey & Genevieve Lakier, *What Are Networks, Platforms, and Utilities and What Should We Do with Them?*, Notice & Comment Blog, YALE J. REG. (Jan. 24, 2023), https://www.yalejreg.com/nc/symposium-networks-platforms-utilities-07/ [https://perma.cc/BV6Y-6GTG] ("Why would a company that earns a steady return from fossil generators voluntarily transition to cheaper and cleaner fuels? But as an example of how public utilities can end up wielding power not in the public interest, it poses a significant challenge to the NPU model.").

[89] *See* Elettra Bietti, *Experimentalism in Digital Platform Markets: Antitrust and Utilities' Convergence*, 2024 U. ILL. L. REV. 101, 131–32.

[90] *See, e.g.*, Andy Yen, *Apple's DMA compliance plan is a trap and a slap in the face for the European Commission*, PROTON BLOG (Feb. 5, 2024), https://www.proton.me/blog/apple-dma-compliance-plan-trap [https://perma.cc/76SW-26U3] (detailing Apple's malicious compliance with the DMA); Casey Newton, *Everything Mark Zuckerberg Has Gotten From Donald Trump So Far*, PLATFORMER (Aug. 28, 2025), https://www.platformer.news/trump-zuckerberg-meta-partnership-eu-dsa-ai-dma/ [https://perma.cc/97D7-E4ML] (detailing Meta's largely successful efforts to get the Trump administration to fight European regulators' on the company's behalf).

[91] *See, e.g.*, Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776, 806–07 (2020).

of the company's revenue.[92] As the Neo-Brandeisians have rightly noted, ignoring this too-big-to-regulate problem perilously invites the incumbents to engage in malicious compliance—at best.[93] So if there's any hope that data-governance policies that overtly regulate firms' data-exploitation practices are to meaningfully change the status quo, we need antitrust law to break up the largest companies and to cultivate markets with smaller, more manageable firms.

A second place for the new antitrust paradigm is a category of data-monetization practices that may be best—or only—governable through increased competitive pressures. For instance, firms large and small are commonly employing data to individualize financial terms with their counterparties.[94] This individualization generally occurs in four spheres: risk-profiling products like credit and insurance; consumer prices and offers; rent; and wages.[95] In each instance, data affords one party the ability to apprehend and predict their counterparty's willingness to buy or sell. There is a long and robust tradition of overtly regulating what types of information may inform credit decisions and insurance prices,[96] which might pave the way for further direct governance. But it will likely be more difficult to directly govern the other spheres affected by individualization, leaving competition policy as the most suitable tool.

Algorithmic wage discrimination is likely to prove especially difficult to directly govern. Zephyr Teachout has explained that outlawing "first degree labor price discrimination is no small task, especially in the United States, where there is a broad culture of allowing employers near absolute discretion in wage setting outside of prohibited

---

[92] *See* Cohen, *supra* note 44, at 19 (citing Nilay Patel, *Facebook's $5 Billion FTC Fine Is an Embarrassing Joke*, THE VERGE (July 12, 2019), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

[93] *See, e.g.*, TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 15 (2018); Zephyr Teachout & Lina Khan, *Market Structure and Political Law: A Taxonomy of Power*, 9 DUKE J. CONST. L. & PUB. POL'Y 37, 37 (2014); *cf.* Yen, *supra* note 90.

[94] *See* Ormerod, *supra* note 11, at 25 nn.172–74.

[95] *Id.*

[96] *See id.* at 31–32.

categories of age, sex, race, and the other limited protected categories."[97] Other avenues for checking employers' power to engage in algorithmic wage discrimination, like labor organization, have long been in retreat.[98] Recalibrating the balance of power between labor and management has been a prominent theme of Neo-Brandeis scholarship, and competition-increasing interventions should reduce employers' ability to dictate dystopian conditions of employment. None of this is to suggest that rules don't have a role to play here: recent pay transparency efforts should be expanded, since the prevailing norm of compensation opacity makes it difficult for employees to compare wages, benefits, and terms of employment.[99] In short, because surveillance-based wages likely cannot be eradicated exclusively through overt regulation and because of monopsonistic labor markets, increasing competition between employers—in tandem with increased transparency—should prove to be an effective tool for policymakers looking to address harmful datafication in the workplace.

Surveillance-based consumer pricing would seem to reside somewhere between risk profiling and wages; both a competition-based and rule-based approach may have their virtues. I have argued that policymakers should enact certain rule-based approaches, namely: outlawing financial personalization based on some categories of data; mandating that firms offer the same prices and discounts to everyone on an equal basis; and requiring that firms inform putative customers about how they can receive the discounted price.[100]

---

[97] Zephyr Teachout, *Algorithmic Personalized Wages*, 51 POL. & SOC'Y 436 (2023).

[98] *See* Bureau of Labor Statistics, *Union Members Summary* (Jan. 28, 2025), https://www.bls.gov/news.release/union2.nr0.htm [https://perma.cc/BK6C-3BXL] (pegging union membership in 2024 at 9.9%, down from 20.1% in 1983); *cf.* Janus v. Am. Fed. of State, County & Munic. Workers, 585 U.S. 878 (2018).

[99] *See* Shengwei Sun, Jake Rosenfeld, and Patrick Denice, *On the Books, Off the Record: Examining the Effectiveness of Pay Secrecy Law*s *in the United States*, INST. WOMEN'S POL'Y RSCH. (Jan. 2021), https://iwpr.org/wp-content/uploads/2021/01/Pay-Secrecy-Policy-Brief-v4.pdf [https://perma.cc/7B4W-XXKH].

[100] Ormerod, *supra* note 11, at 44.

California lawmakers recently proposed a ban on individualized pricing, though the bill stalled after being narrowed to grocery prices.[101] But even if the effort had succeeded, it included an inoculation when the seller disclosed the individualization and obtained the customer's putative "written affirmative consent"—the exact same notice-and-choice paradigm that undergirds legions of ineffective privacy laws. Increasing competition might therefore accomplish what rules alone cannot: harnessing consumers' visceral antipathy for personalized pricing to incentivize firms to eschew it.[102] Pairing a competitive market with effective disclosure requirements could thus prove to be a powerful combination. Upon being informed that a retailer is personalizing financial terms, consumers are likely to balk and look for a competitor that doesn't.

To be sure, the strategy has its perils since transparency requirements impose decisional fatigue on individuals. But I think competitive pressure holds more promise when dealing with matters of dollars and cents rather than opaque, easily obscured data practices. If there is anywhere that policymakers

---

[101] *See* Rachael Myrow, *California Lawmakers Take on Predatory 'Surveillance Pricing'*, KQED (Feb. 26, 2025), kqed.org/news/12028137/california-lawmakers-take-on-predatory-surveillance-pricing; Roma Patel, *The Price You Pay: California Largely Strikes Down Bill Banning Surveillance Pricing*, NAT'L L. REV. (Sept. 4, 2025), https://natlawreview.com/article/price-you-pay-california-largely-strikes-down-bill-banning-surveillance-pricing [https://perma.cc/JU2V-LTGB].

[102] *See* Joshua Rhett Miller, *Outrage Grows as Delta to Price Tickets Based on What AI Thinks You'll Pay*, NEWSWEEK (July 22, 2025), https://www.newsweek.com/senators-want-answers-delta-ai-powered-pricing-plan-2102358 [https://perma.cc/L78N-VQND]; Julian Runge, *Getting ML-Based App Personalization Right: The Engagement Engineering Framework*, MOBILE DEV MEMO (Feb. 21, 2023), https://www.mobiledevmemo.com/getting-ml-based-app-personalization-right-the-engagement-engineering-framework/ [https://perma.cc/2BX8-9E53] ("Price personalization is largely a no-no in gaming where large and engaged communities do not take it well when companies try to charge different prices for one and the same good."); Lee Anne Fennell, *Optional Price Discrimination*, 10 TEX. A&M L. REV. 485, 486 (2023) ("Price discrimination gets a bad rap. It is associated with the exploitation of monopoly power and with opportunistically extracting surplus from consumers.").

can rely on consumers voting with their business to indirectly discipline unsavory business practices, personalized pricing would seem to be it.

Competition policy may also have a place in markets where high levels of concentration enable coordinated behavior. Surveillance pricing and algorithmic rent provide apt illustrations. The FTC recently released a preliminary study into surveillance-based pricing practices.[103] The study, which was the byproduct of sending requests for information to just eight companies,[104] shows how hundreds of individual retailers farm out the work of algorithmically modulating prices to a small handful of data processors.[105] The Biden administration also brought an antitrust enforcement action against RealPage for monopolizing the market that landlords use to price apartments, arguing that it facilitated price coordination among landlords who would otherwise compete.[106] A highly consolidated market of intermediaries, in other words, enables and unlocks a host of abusive business practices that may be more difficult to sustain in the absence of concentration.

Tension between promoting competition and enabling user control over data is unavoidable here. Pro-competitive policies that diffuse these intermediaries' power will almost by

---

[103] *See FTC Surveillance Pricing 6(b) Study: Research Summaries & A Staff Perspective,* FED. TRADE COMM'N (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf [https://perma.cc/Q8C6-A4AD].

[104] *See* Press Release, *FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing*, FED. TRADE COMM'N (July 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing [https://perma.cc/2GBJ-H7VH].

[105] *See FTC Surveillance Pricing 6(b) Study: Research Summaries & A Staff Perspective*, *supra* note 103, at 7.

[106] Press Release, *Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters*, DEPT. OF JUSTICE (Aug. 23, 2024), https://www.justice.gov/archives/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters [https://perma.cc/NDR5-XEFG]; Council of Economic Advisors*, The Cost of Anticompetitive Pricing Algorithms in Rental Housing*, THE WHITE HOUSE (Dec. 17, 2024), https://bidenwhitehouse.archives.gov/cea/written-materials/2024/12/17/the-cost-of-anticompetitive-pricing-algorithms-in-rental-housing/ [https://perma.cc/Y4KH-3FVN].

definition further extend data flows.[107] Google, for instance, has recently been compelled to share its search index with competitors.[108] This approach is a potent tool for increasing competition in web search, but it's also undeniable that it would further alienate users from their data. Policymakers may nevertheless conclude that this is an acceptable trade-off if doing so makes it more difficult or impossible for companies to engage in at least some forms of unsavory conduct.

In sum, despite the frictions between them, policymaking in the coming decades must recognize that antitrust and data-governance law should work in tandem: breaking up data intermediaries *and* prescribing permissible data practices will be necessary to effectively ameliorate both the individualized and collectivist harms of datafication.

Conclusion

Policymakers navigating the interplay between competition policy and data governance must recognize that neither can be a panacea. In isolation, structural data-governance interventions hold more promise for disciplining firms' data exploitation practices than competition policy does, because competitive pressure alone rarely produces meaningful improvement in firms' data activities. But since data regulation tends to advantage existing firms, competition law will be necessary to limit the size and influence of today's data-processing behemoths, and it may prove useful in other realms where overt regulation is likely to prove futile. Mediating the tensions between these renewed regulatory approaches will

---

[107] *Cf.* Ormerod, *supra* note 2, at 218–19 n.215 (grappling with the question of whether extending data flows in this fashion actually exacerbates a "privacy" problem).

[108] *See* United States v. Google, 2025 WL 2523010 (Sept. 2, 2025); Karina Montoya, *Analyzing Week One of Google Search's Antitrust Remedies Trial*, TECH POL'Y PRESS (Apr. 29, 2025), https://www.techpolicy.press/analyzing-week-one-of-google-searchs-antitrust-remedies-trial/ [https://perma.cc/9PNE-LZL9]; The Talk Show, "*A Professional Internet User,"* DARING FIREBALL, at 01:09:45-01:23:33 (Dec. 24, 2024), https://www.daringfireball.net/thetalkshow/2024/12/24/ep-416 [https://perma.cc/DLK5-X5SG] (discussing nationalizing Google's search index).

prove essential to distributing power more equitably in our information age.