PRIVACY PRETEXTS

Rory Van Loo†

Data privacy's ethos lies in protecting the individual from institutions. Increasingly, however, institutions are deploying privacy arguments in ways that harm individuals. Tech companies like Amazon, Meta (Facebook), and Alphabet (Google) wall off information from competitors in the name of privacy. Financial institutions under investigation justify withholding files from the Consumer Financial Protection Bureau by saying they must protect sensitive customer data. In these and other ways, the private sector is exploiting privacy to avoid competition and accountability. This Article highlights the breadth of privacy pretexts and uncovers their moral structure. Like most pretexts, there is an element of truth to the claims. But left unchallenged, they will pave a path contrary to privacy's ethos by blocking individuals' data allies—the digital helpers, competitors, and regulators who need access to personal data to advance people's interests. Addressing this move requires recognizing and overcoming deep tensions in the field of privacy. The field's normative relationship with economics and third-party access has become too strained. Although data privacy's roots are in guarding against access, its future depends on promoting allied access.

---

† Boston University School of Law and Affiliated Fellow, Yale Law School Information Society Project. For valuable comments on prior drafts, I am grateful to Joseph Blocher, Jamie Boyle, Molly Brady, Christopher Conley, Rebecca Crootof, Nita Farahany, Eric Fish, Meirav Furth-Matzkin, Talia Gillis, Woody Hartzog, Hiba Hafiz, Scott Hirst, David A. Hoffman, Howell Jackson, Gary Lawson, Daniel Markovits, Florencia Marotta-Wurgler, Christopher Morten, Manisha Padi, Nicholas Parrillo, Robert Post, Shitong Qiao, Arti Rai, Christopher Robertson, Andy Sellars, Jessica Silbey, David Walker, Ryan Williams, Jonathan Wiener, Ramsi Woodcock, and Felix Wu. The Article also benefitted greatly from comments by workshop participants at Boston College, Boston University, Cardozo, Duke University, New York University, the University of Connecticut, and the Wharton School at the University of Pennsylvania. Victoria Abramchuk, Emma Burnett, Celene Chen, Karen Clarke, Samuel Cournoyer, Liam Cronan, Jamie Donnelly, Brian Flaherty, and Joe Long contributed excellent research assistance and edits.

INTRODUCTION

Seeking to fend off competitive upstarts, Facebook blocked fast-growing apps' access to user data while publicly explaining the move as necessary to safeguard users' privacy.[1] After thousands of customers fell victim to fraud, Western Union fought a Federal Trade Commission (FTC) demand for information by arguing that "privacy laws in 55 countries would be implicated if it complied."[2] Sued for malpractice, Kaiser Permanente—one of the nation's largest healthcare providers—resisted producing information about the plaintiff's own medical files by arguing that it was prohibited from doing so under the Health Insurance Portability and Accountability Act (HIPAA), the leading health privacy statute.[3]

---

[1] *See Read the Leaked Facebook Documents*, NBC NEWS, https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents [https://perma.cc/MN7E-Y2EF] (select "Sealed exhibits") (last visited Oct. 9, 2022) [hereinafter *Facebook Leaked Documents*]; *infra* subpart II.A.

[2] Brief for Appellee and Cross-Appellant at 38, FTC v. W. Union Co., 579 F. App'x. 55 (2d Cir. 2014) (Nos. 13-3100, 13-3272).

[3] Defendant's Response in Opposition to Plaintiff's Motion to Compel Portions of the Audit Trail Withheld by Defendant & Request for Sanctions at 3, Ortega v. Colo. Permanente Grp., P.C., No. 2009-cv-9328, 2010 WL 8753150 (Colo. Dist. Ct. Nov. 29, 2010) 2010 WL 8880811 (asserting that "HIPAA

In these and many similar instances, large institutions—including Alphabet (Google), Amazon, Apple, Capital One, and Bank of America—turn privacy on its head. At its modern core, information privacy is animated by holding institutions accountable to individuals.[4] Yet businesses are systematically citing privacy to advance their interests at the expense of individuals.[5] Such behavior is problematic because it shows how businesses can opportunistically use privacy to weaken markets and the rule of law.

This Article shows the extent of this weaponization of privacy against the information economy.[6] I and others have previously discussed the use of privacy as an excuse to undermine competition to block third-party digital tools seeking to help consumers shop,[7] as a procedural move to

---

regulations expressly deny Plaintiff the right to request an accounting of internal uses and disclosures" of the Plaintiff's health file).

4 This is true for both the federal government and private companies. *See infra* subpart I.A. (summarizing privacy statutes).

5 Note that there may still be a privacy interest advanced. *See infra* subpart I.A. This differs from how businesses have exploited the weak privacy legal regime, which involves circumventing privacy laws to extract data rather than repurposing them to block data. For valuable analyses of businesses manipulating or disingenuously bypassing privacy laws, upon which this Article builds, see, for example, JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 5–8, 56–58, 262 (2019), which explains that the problems with a weak privacy framework, in particular how the notice-and-consent regime presents "opportunities for co-optation by corporate claimants," and Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 834 (2020), which concludes that "paper trails, assessments and audits, internal and external policies, to name just a few—take the place of actual adherence to [privacy] law."

6 For a more straightforward consideration of whether businesses can legitimately assert their own privacy interests, see, for example, Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27, 29 (2014), which notes that "scholars have all but overlooked whether a corporate constitutional right to privacy exists."

7 *See* Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 242–43 (2018) [hereinafter Van Loo, *Making Innovation More Competitive*] (noting that businesses misappropriate security laws to justify anticompetitive blocking of fintechs); Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 837–39 (2019) [hereinafter Van Loo, *Digital Market Perfection*] (urging skepticism of privacy claims used to block digital intermediary acquisition of information); Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951 (2021) (discussing how tech platforms misuse questionable privacy arguments). Facebook also paid for an analysis of Apple's emphasis on privacy in blocking data for Facebook and others. *See* D. Daniel Sokol & Feng Zhu, *Harming Competition and Consumers Under the Guise of Protecting Privacy*: *An Analysis of Apple's iOS 14 Policy Updates* (June 14, 2021), https://ssrn.com/abstract=3852744 [https://perma.cc/8K4J-PPYW]. For sustained treatments of antitrust and privacy from the perspective of seeing the need to elevate genuine privacy concerns, see Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. F. 647, 654, 661 (2021)

block a criminal defendant from obtaining exculpatory information,[8] and as a "pretext" for deregulation.[9] These prior explorations of data privacy misuse are individually important, but their disconnect obscures the potential scope of the problem.[10] Widening the lens to link widespread instances of businesses using privacy to block market and regulatory information not only shows the breadth of the problem but also helps to unpack privacy pretexts' normative architecture, revealing deep dysfunctions in the data governance framework.[11]

To see privacy pretexts' moral architecture, it helps to surface the underlying norms. Early conceptions of information privacy emphasized an anti-intrusion impulse as reflecting a desire "to be let alone" by not being watched or having some information kept secret.[12] Applied to data, this and related conceptions of privacy focus attention on safeguarding the individual from the threat of unwanted access to information.[13] It is this early, visceral anti-intrusion notion of privacy that businesses channel when they deploy

---

(proposing greater weight be given to privacy matters in antitrust); Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 86 (2019). Finally, scholars have long grappled with a broader point, that privacy sits in tension with the free flow of information, and that privacy involves tradeoffs, most notably with freedom of speech. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 353, 359–61 (1967) (observing that privacy faces challenges due to the embrace of the free flow of information); NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 27–40 (2015) (summarizing the tension between privacy and free speech); Van Loo, *Digital Market Perfection*, *supra*, (urging skepticism of privacy claims used to block digital intermediary acquisition of information).

8 Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2722 (2021) (analyzing businesses' use of privacy to withhold potentially exculpatory evidence from criminal defendants); *see also* Kiel Brennan-Marquez, *Beware of Giant Tech Companies Bearing Jurisprudential Gifts*, 134 HARV. L. REV. F. 434 (2021) (casting Wexler's argument as a broader gambit).

9 *See* Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1563 (2019) [hereinafter Van Loo, *The Missing Regulatory State*] (arguing that privacy arguments are increasingly undermining regulatory monitoring of businesses).

10 Indeed, a broader information-limiting function of the law may be observed, if privacy were combined with other areas of the law, such as intellectual property. *See infra* note 233.

11 For a helpful framing of data governance, see Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 586 (2021).

12 Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2164, 2166 (2003); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1419–30 (2001).

13 *See* Solove, *supra* note 12, at 1419–30.

privacy pretexts to advance their own interests.

Yet people have a distinct set of interests in what a business does with their data even if the business rightfully has accessed it and never spreads it.[14] For instance, people may accept that Facebook collects data about them but not want that data to be used to discriminate against them or to manipulate their decisions. And they may not want their data to be used to charge them monopoly prices. That other set of interests people have in institutions responsibly managing their data is referred to hereinafter as data management.[15]

The core move businesses make in privacy pretexts is to use fundamentalist anti-intrusion norms as a smokescreen to cover for a violation of data management norms. For example, the Computer Fraud and Abuse Act (CFAA) was intended to keep hackers out of computers.[16] In other words, the CFAA protects against intrusions. Yet for years, platforms like Facebook and Amazon have convinced judges that the CFAA allows the platforms to sue third-parties that collect even publicly available data.[17] The businesses that Facebook, Amazon, and other incumbents targeted included startups that helped people save money on everything from auto rentals to online shopping.[18] Many of these startups rapidly failed or became far less helpful to consumers because the CFAA lawsuits deprived them of essential information, even though

---

14 *See, e.g.*, Katherine J. Strandburg, *Monitoring, Datafication and Consent: Legal Approaches to Privacy in the Big Data Context*, *in* PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 11 (Julia Lane et al. eds., 2014) (noting that the "development of digital computers . . . raised fears of misuse . . . distinct from the concerns about emotional distress and reputation at the heart of the privacy torts").

15 This term is adopted, despite limits, for lack of an agreed upon term in the literature. Its meaning is expanded upon *infra* Part I.

16 18 U.S.C. § 1030; Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (explaining how the CFAA followed a period in which "a series of highly publicized hackings captured the public's attention"). On the CFAA as a privacy law, see, for example, Leslie R. Caldwell, *Prosecuting Privacy Abuses by Corporate and Government Insiders*, U.S. DEP'T OF JUST. ARCHIVES (Mar. 16, 2015), http://www.justice.gov/archives/opa/blog/prosecuting-privacy-abuses-corporate-and-government-insiders [https://perma.cc/K9DQ-ZM49], which describes the CFAA as "the law that protects the privacy and security of computer owners and users."

17 *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065–69 (9th Cir. 2016) (holding third-party platform liable under CFAA for accessing Facebook users' data "without authorization"). Although scholars have persuasively argued against this statute's misinterpretation, those conversations have not diagnosed the CFAA as part of a broader misappropriation of privacy against markets. Orin Kerr is the leading voice on the CFAA's misuse. Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016).

18 *See infra* subpart II.A.

consumers wanted them to have the information.[19] Privacy pretexts thereby enabled tech companies to twist an anti-intrusion statute into a statute that made consumers pay higher prices or become more dependent on the largest platforms.

This gambit works partly because anti-intrusion is far more normatively salient. The impulse to resist intrusion has a centuries-long head start in its development. The common law protects against an invasion of privacy, and the Fourth Amendment prohibits unreasonable searches.[20] Modern scandals have further elevated anti-intrusion sentiments in the public consciousness. Equifax, a credit reporting agency, compromised about 150 million consumers' social security numbers, and Facebook gave Cambridge Analytica access to the data of over 70 million unwitting users, which the political consulting firm used to micro-target ads for the 2016 presidential election.[21] In contrast, data management is newer and guards against harms that are less instinctually alarming.[22] Thus, privacy pretexts pit a well-developed and visceral normative foundation for anti-intrusion against a more recent and subtle set of interests in data management.

Ironically, privacy scholars have moved beyond the view of privacy as only guarding against intrusions to safeguard secrecy or reputation.[23] A vast and vibrant literature has also argued that privacy serves to advance autonomy, fair information practices,[24] equality,[25] civil society,[26] deliberative democracy,[27] liberal citizenship, and human flourishing,

---

19 *See* Van Loo, *Digital Market Perfection*, *supra* note 7, at 837–39 (summarizing incumbents' strategic blocking of data).

20 U.S. CONST. amend. IV.

21 McKenzie L. Kuhn, Note, *147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches*, 104 IOWA L. REV. 417, 419 (2018).

22 *See infra* Part I (summarizing data management's statutory development).

23 *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 149–50 (2012) ("Privacy is not only about refusing access, visibility, or interference with particular decisions. It is also and more generally about preventing the seamless imposition of patterns predetermined by others."); Schwartz & Treanor, *supra* note 12, at 2164 (distinguishing the old privacy from the new).

24 *See, e.g.*, Schwartz & Treanor, *supra* note 12, at 2164 ("The new privacy is centered around Fair Information Practices ('FIPs') . . . .").

25 *See* Radhika Rao, *A Veil of Genetic Ignorance? Protecting Genetic Privacy to Ensure Equality*, 51 VILL. L. REV. 827 (2006). *See generally* PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

26 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989).

27 Paul M. Schwartz, *Privacy and Participation: Personal Information and*

among other goals.[28] Scholars agree on neither how privacy is to be defined nor whether it is even worth talking about the field's boundaries, and this Article adopts no definition.[29] But viewing privacy through these newer and expanded lenses means that data management practices are valuable for advancing those goals.[30] Additionally, many of the newer definitions of privacy would include significant parts of data management, at least in the sense that many view data protection as part of data privacy.[31] For those holding such a view, privacy pretexts involve pitting one face of privacy against another.

Regardless of privacy's boundaries, understanding the normative architecture deployed by privacy pretexts is important because it indicates the need for deeper renovations to the information governance framework. Most importantly, privacy has traditionally emphasized restrictions on third-party access to prevent incidents such as the Equifax breaches and the Cambridge Analytica scandal.[32] But the goals of data management cannot be advanced solely by restricting access. Indeed, they depend on third-party access. Modern markets are so complex that skillfully navigating them requires consumers to have guidance from digital helpers, such as price comparison engines and online financial

---

Public Sector Regulation in the United States, 80 IOWA L. REV. 553, 556, 557, 560 (1995) (putting forth a conception of privacy as related to deliberative democracy and deliberative autonomy, "which concerns the underlying capacity of individuals to form and act on notions of the good when deciding how to live their lives").

28 *See, e.g.*, Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1927 (2013) ("Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy.").

29 *See, e.g.*, Robert C. Post, *Three Concepts of Privacy*, GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."); Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1688 (2021).

30 *See infra* Part IV. Privacy theorists have often argued against simplifying privacy and making it one-dimensional. *See, e.g.*, COHEN, *supra* note 23, at 152 ("Human flourishing requires both boundedness and some ability to manage boundedness.")

31 Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 98, 101 (2020) ("Data protection is more akin to what many in the United States call 'data privacy' or 'information privacy': protections that attach to data sets (of personal data) that are stored and analyzed en masse."). This conceptual overlap will seem perplexing to some, and the resulting confusion raises some interesting issues explored below. *See infra* Part I.

32 *See infra* Parts I, III.

calculators.[33] However, to make effective decisions, those digital tools require access to data about the individual. Another category of crucial third-party access comes from regulators. Many data management harms would be difficult, if not impossible, for individuals to discover on their own, such as whether banks are using information about an applicant's race or gender to set loan rates.

Access by regulators and digital helpers is thus essential to data management. Yet privacy's dominant normative skepticism of third-party access helps set up businesses to use pretexts to reframe beneficial third-party access as an intrusion on the customer. To make that move less effective, this Article proposes that privacy norms emphasize allied access. Allied access means systematically identifying contexts in which the sharing of data with third parties might increase accountability, competition, and user sophistication.[34]

Harmonizing anti-intrusion and allied access requires addressing another normative feature that privacy pretexts exploit: the subversion of economics. Privacy scholars have often sought to de-emphasize economic considerations.[35] That stance is understandable because economic arguments have long provided fierce opposition to privacy regulation, based largely on the costs of such regulation and the harms that would result to innovation.[36] Yet some of the most widely supported justifications for data management lie in economics, in terms of both efficiency and distributive justice.[37] By paying insufficient attention to these prongs of economic analysis, privacy has left an opening for privacy pretexts to focus attention away from data management's economic harms toward a visceral intrusion benefit, claimed by the business, in cutting off data access to third parties.

These conceptual takeaways have important policy implications. Lawmakers and regulators should write and enforce legal rules with privacy pretexts in mind. Mindfulness does not mean weakening important anti-intrusion legislation,

---

33 *See, e.g.*, Oren Bar-Gill & Rebecca Stone, *Pricing Misperceptions: Explaining Pricing Structure in the Cell Phone Service Market*, 9 J. EMPIRICAL LEGAL STUD. 430, 454–55 (2012) (showing how behavioral economics complicates pricing).

34 This concept draws on diverse foundational conceptions in the literature, and thus is arguably as much positive as it is prescriptive. *See infra* Part III.

35 *See infra* section III.B.2.

36 *Id.*

37 These economic harms have been the object of attention by scholars outside of privacy. *See infra* section III.B.2.

but rather remaining vigilant about preserving allied access when writing rules. It also means considering how the misappropriation of any given privacy law might undermine data management interests. Additionally, adopting that privacy misappropriation lens would help to identify existing laws, such as the CFAA, whose reform would advance allied access.[38] Although not the focus of this Article, doctrines outside of privacy, such as consumer law and antitrust, could also benefit from recognizing privacy pretexts and could play a role in developing allied access.[39]

Now is a particularly important time to scrutinize privacy pretexts because we are in the midst of a "constitutional moment" for privacy,[40] one of those rare times when "We the People" engage with enough vigor to potentially push large-scale legal change.[41] If a once-in-a-generation federal privacy statute is enacted, it may then be too late to start looking at pretexts. It is hard to imagine follow-up legislation just to address the problem of pretexts.[42] Either way, privacy law continues to develop at the state level and through federal administrative agencies.[43] Businesses have long shown great skill at mobilizing laws ranging from free speech to trade secrets as a form of Lochnerism to block regulation and wall off public information.[44] Strong privacy laws are crucial, but

---

38 Recent cases have taken steps in this direction. *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021) (narrowing the scope of "unauthorized access" under the CFAA).

39 Consumer protection laws prohibit some misleading statements by businesses, and antitrust generally aims to block anticompetitive conduct. In theory, some privacy pretext examples could be addressed by those doctrines. Moreover, each of these areas engages in balancing tests that would be sharpened by not falling for privacy pretext arguments. This Article focuses on other solutions because such implications are at best a small part of the solution. *See infra* Part IV.

40 Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1692 (2020).

41 *See* BRUCE ACKERMAN, WE THE PEOPLE: FOUNDATIONS 6–7 (1991) (developing the concept of constitutional moment).

42 Among other reasons, firms will build around the privacy legislation. It may then no longer be cost-effective to reengineer the system to allow regulatory inspection without exposure to extensive personal data.

43 *See, e.g.*, Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) (describing FTC privacy enforcement).

44 *See* JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 13 (1996) ("Sometimes the technologies, art forms, and commercial practices that succeed are those that fit a particular set of legal metaphors."); COHEN, *supra* note 5, at 5–8 ("Law for the information economy is emerging . . . via the ordinary, uncoordinated but

designing them without an eye toward ways that incumbent businesses might manipulate them risks providing industry with more powerful weapons of information control. Safeguards against pretexts should be integrated into the blueprints while the privacy framework is still substantially under construction.

Understanding privacy pretexts is thus valuable for the challenging task of maximizing the returns that information markets bring to society. Moreover, because addressing privacy's obfuscation of data management would yield economic benefits, the improved normative architecture could provide intellectual foundations for a stronger coalition in support of omnibus privacy legislation. Identifying the widespread repurposing of privacy thus sheds light on a clearer path toward seizing the current constitutional moment—and doing so in a way that moors privacy law to its purpose of protecting individuals rather than institutions.

The Article proceeds as follows. Part I outlines the origins of information privacy, paying particular attention to the development of anti-intrusion and data management statutes. Part II shows the breadth of businesses leveraging privacy pretexts to block information from both private actors and regulators. Part III uncovers the normative architecture of privacy pretexts, showing how they benefit from the subversion of economics and ambivalence about third-party access.

---

self-interested efforts of information-economy participants and the lawyers and lobbyists they employ."); Jonathan B. Wiener & Barak D. Richman, *Mechanism Choice*, *in* RESEARCH HANDBOOK ON PUBLIC CHOICE AND PUBLIC LAW 373–74 (Daniel A. Farber & Anne Joseph O'Connell eds., 2010) (summarizing the literature on how industry may for its own interests influence the regulatory process); Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 464 (1998) (observing that "the economic vision embodied in *Lochner* is alive and well" in intellectual property law); Lochner v. New York, 198 U.S. 45, 62 (1905) (striking down laws limiting working hours as unreasonable restrictions on contract); Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133, 206 ("The new *Lochner*'s absolutist 'speech is speech' argument must be rejected . . . ."); Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383, 392–93 (2017) (observing that "changing the legal environment is crucially important," an "increasingly salient" practice, and a "material part of the business plan" for some companies); David E. Pozen, *Transparency's Ideological Drift*, 128 YALE L.J. 100, 140 (2018) (arguing that transparency has evolved from its roots in progressive purposes to advance a deregulatory agenda); Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. DAVIS L. REV. 1367 (2022); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1279 (2019) ("[T]rade secrecy's dominance over source code has been a significant cause for concern in cases involving the public interest."); Christopher J. Morten, *Publicizing Corporate Secrets*, 171 U. PA. L. REV. (forthcoming 2022), https://papers.ssrn.com/abstract=4041556 [https://perma.cc/2D2M-BNVL].

Part IV sketches normative implications. The most promising reforms lie not in punishing pretexts but in promoting data management. In particular, a strong allied access principle and greater attention to economic interests would lessen the chances that conceptual blind spots enable privacy to serve as an instrument for eroding markets and democracy.

Before turning to the main discussion, two brief notes are in order about terminology. First, despite the focus on data, the Article's broader privacy pretexts framing is meant to signal the scope and stakes of the problem. Scholars have previously called attention to the use of privacy as a "pretext" not only in narrower data contexts,[45] but also in highly specific non-data contexts. For instance, Susan Hazeldean and others have argued that some use privacy as a "pretext" to fight the law's evolution regarding gender identity and sexual orientation.[46] It is worth exploring whether a related move is at play in these non-data contexts of pitting the old privacy against the new. Regardless, the stakes of privacy pretexts go beyond what many people presumably imagine when they think about data.

Second, the word pretext has different implications. In its most basic form, a privacy pretext occurs when the business states that it is doing something for privacy purposes, but its main motivation for that conduct really comes from something else. Privacy pretexts may involve mixed motives.[47] In many cases, at least some constituents within the business might be motivated to improve privacy, even if the main decisionmakers' motives are something else. In other cases, the business may not actually be motivated by privacy at all. Because determining corporate motive is notoriously difficult, the case for a privacy pretext is usually circumstantial. But blurred boundaries surrounding the definition of pretexts should not be allowed to get in the way of the more important observation.

---

45 *See, e.g.*, Van Loo, *The Missing Regulatory State*, *supra* note 9.

46 *See, e.g.*, Susan Hazeldean, *Privacy as Pretext*, 104 CORNELL L. REV. 1719, 1721 (2019) ("An asserted need to safeguard women's privacy has become a rallying cry for the opponents of laws forbidding discrimination based on gender identity or sexual orientation."); Ruth Colker, *Public Restrooms: Flipping the Default Rules*, 78 OHIO ST. L.J. 145, 164 (2017) ("The privacy justification is actually a pretext for the articulation of gender stereotypes about the inappropriateness of men being exposed to women's private, bodily functions."). For an example of prior references to privacy pretexts in the informational context, see Van Loo, *The Missing Regulatory State*, *supra* note 9. I am grateful to Susan Hazeldean for her help in navigating the similar titles in the same journal.

47 Mixed motives create a difficult challenge that the law handles inconsistently. Andrew Verstein, *The Jurisprudence of Mixed Motives*, 127 YALE L.J. 1106, 1114 (2018).

Regardless of where on the pretextual spectrum any given example may lie, the systematic inconsistencies and opportunistic deployment of privacy arguments pose a problem when the harms from the hidden interests advanced substantially outweigh the highlighted privacy gains.

I
PRIVACY'S NORMATIVE IMBALANCE

This Part sketches the two faces of privacy pretexts: anti-intrusion and data management. Anti-intrusion safeguards personal information from unwanted data access, acquisition, or dissemination. We may not want Facebook to know us too well, or we may not want our every move to be tracked by Apple and Google through our phones. Once an institution collects our data, we may not want them to sell it, and most of us certainly would not want them to let hackers steal it.[48] Guarding against unwanted intrusions or surveillance is an important component of privacy.

A second set of interests implicated by privacy pretexts can be summarized as about data management. Data management is used here to refer to the diverse set of interests that people have in their data beyond intrusions. It focuses on how institutions use information once they have access. Its more individual component would prevent the institution from using data in a way that harms the subject of the data, such as when prices are discriminatorily inflated on the basis of race, gender, or other identified characteristics. Another example of a harm is the use of data to manipulate the data subjects' decisions, such as in purchasing or voting.[49]

Data management also captures a more collective goal of maximizing the societal gains from personal data. Efficiency is one such collective interest; the data collected should be managed in a manner that encourages competitive prices and

---

[48] Scholars and practitioners have approached the question of whether to include data security within privacy in different ways. *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (treating privacy issues and data breaches as interchangeable); Lauren Henry, *Information Privacy and Data Security*, 2015 CARDOZO L. REV. DE NOVO 107, 107 ("Data security has separate objectives from information privacy that can be agnostic or even in opposition to information privacy.").

[49] *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1027–29 (2014) (identifying various economic harms, such as manipulation and rent extraction, using people's data); Solove, *supra* note 12, at 1393–98 (encouraging a more database-oriented approach to privacy).

product choices.[50] Similarly, we may have an interest in our social media data not being used to manipulate other people's votes and thereby undermine democracy—even if our own vote is not being manipulated. Those more collective goals are akin to natural resources management, which requires balancing mineral extraction with tourist access—except here the resource being managed is data.[51] Data management has significant overlap with, but is broader than, data protection, which tends to have a more individual focus.

This Article takes no stance on the proper boundaries of privacy and whether data management should be classified as inside or outside of privacy. Nor does this discussion of anti-intrusion and data management capture the full spectrum of privacy's articulated goals, such as those related to dignity, citizenship, and power, or how to achieve them. Privacy has a "bewildering variety of meanings."[52] Privacy scholars have argued that attempts at defining privacy risk ending up distracting readers and thus getting in the way of progress.[53] This anti-intrusion versus data management taxonomy is offered to illuminate some of the main norms involved in privacy pretexts, not to offer a comprehensive treatment of privacy.[54]

Nonetheless, it is undeniable that many scholars and laws classify significant parts of data management interests as privacy.[55] That classification is particularly prominent in the

---

50 Note that the interests in anti-discrimination and anti-manipulation can be viewed from a collective perspective, in the sense of wanting to promote societal equality or prevent meddling in elections.

51 For conceptions of privacy that explore analogies to natural resources, see Dennis D. Hirsch & Jonathan H. King, *Big Data Sustainability: An Environmental Management Systems Analogy*, 72 WASH. & LEE L. REV. ONLINE 406, 407 (2016); COHEN, *supra* note 5, at 48–49.

52 RICHARDS, *supra* note 7, at 8.

53 *See, e.g.*, HELEN FAY NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 7–12 (2010) (pointing out that focusing on the definitional debates gets in the way of progress); Hartzog, *supra* note 29, at 1688 (emphasizing the importance of "shifting our focus away from questions about what privacy is and toward the different problems we want our privacy-based rules to address and the specific values we want them to serve"). *But see* Jeffrey Bellin, *Pure Privacy*, 116 NW. U. L. REV. 463, 471 (2021) (proposing a baseline definition of the terms "right to privacy" and "privacy" to anchor legal privacy discourse).

54 *See, e.g.*, NISSENBAUM, *supra* note 53 (declining to adopt any particular definition of privacy).

55 For examples of scholars who have this broader view of privacy, see Hartzog & Richards, *supra* note 40, at 1721 (proposing a comprehensive approach to privacy that includes data protection but also includes data externalities, such as the negative effects on democracy); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 489–491 (2006) (laying out 16

U.S., where data privacy often includes data protection.[56] In this and other ways, privacy pretexts involve repurposing an older and more fundamentalist conception of privacy against newer conceptions of data privacy.

Where one comes out on how to classify data management is of no consequence for this Article's core thesis that businesses are systematically weaponizing anti-intrusion norms in ways that undermine an important newer set of economic and social interests related to data. Regardless of privacy's boundaries, understanding privacy pretexts' normative dimension reveals important dysfunctions in the information governance framework.

A. The Norms of Data Privacy Law

An overview of privacy's historical development helps elucidate how businesses use anti-intrusion to weaken data management. Prominent early scholarship on privacy warned of unwelcome technological intrusions. In 1890, when Samuel Warren and Louis Brandeis wrote *The Right to Privacy*—to some, "the most influential law review article of all time"[57]—they were motivated by "inventions and business methods."[58] They situated privacy within an expansive "right 'to be let alone,'" finding doctrinal support in a common law collection of torts guarding against an "intrusion upon the domestic circle."[59] They warned that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices

---

elements of privacy, including aggregation, identification, secondary use, exclusion, increased accessibility, appropriation, distortion, and decisional interference). The American Law Institute's leading publication on the topic, whose reporters were Paul M. Schwartz and Daniel J. Solove, also puts data management as part of privacy. *See* PRINCIPLES OF THE L.: DATA PRIVACY § 1 (AM. L. INST. 2020). For an example of lawmakers viewing data management as part of privacy, see, CAL. CIV. CODE § 1798.100 (2018) (including in the California Consumer Privacy Act a data portability requirement). As another indication of the common inclusion of data management in privacy, the field's leading gathering brings data management scholarship clearly into its fold, albeit with a self-described broad definition of privacy. *See PLSC History*, Privacy Law Scholars Conference, https://privacyscholars.org/plsc-history [https://perma.cc/8PSB-56NA] (last visited Oct. 9, 2022). For a broader treatment of data management, and examples of privacy scholars seeing this as within their field, see *infra* Part I.

56 *See* Jones & Kaminski, *supra* note 31, at 101.

57 *See* CHARLES O. GREGORY & HENRY KALVEN, CASES AND MATERIALS ON TORTS 883 (Little Brown & Co. 1959).

58 Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 193, 195 (1890).

59 *Id.* at 195–96.

threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[60]

Seventy years later, *The Right to Privacy* influenced the first publication to galvanize the public's attention on technological threats to privacy. In 1964, Vance Packard's best-selling book, *The Naked Society*,[61] sparked an eruption in worry about data privacy.[62] It warned that concealed cameras, filing systems, and other new technologies "tend to annihilate the privacy and dignity of citizens under scrutiny."[63] Explicitly adopting the Warren and Brandeis definition of privacy as "the right to be let alone," Packard criticized a broad array of business and government practices, ranging from credit report firms to government wiretapping.[64]

Whereas *The Right to Privacy* had not mentioned the U.S. Constitution or framed itself in norms of government oppression, *The Naked Society* evoked George Orwell's dystopian *1984* world and criticized the Supreme Court for not enacting more robust constitutional protections.[65] The book thereby tied privacy to a set of anti-intrusion norms—most directly, from the Fourth Amendment—that resonated even more deeply with the public than had the common law.[66] Packard's popular writings are credited with prompting Congress to convene a Special Subcommittee on the Invasion of Privacy, and with inspiring privacy advocates who would shape legislation in the ensuing decade.[67]

Despite that strong anti-intrusion core to privacy, in the background, a set of data management interests emerged. Most importantly, in 1973, the Secretary of the Department of Health, Education, and Welfare responded to public concerns by ordering a study of the risks of record-keeping practices.[68] The report outlined a set of *fair information practices* that would

---

60 *Id.* at 195.

61 VANCE PACKARD, THE NAKED SOCIETY 34 (1964).

62 *See* MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 120 (2019); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 151 (2004).

63 PACKARD, *supra* note 61.

64 *Id.* at 34, 223.

65 *See id.* at 21–24.

66 U.S. CONST. amend. IV.

67 Margaret O'Mara, *The End of Privacy Began in the 1960s*, N.Y. TIMES (Dec. 5, 2018), https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html?smid=url-share [https://perma.cc/8JGW-BMNH].

68 U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SEC'YS ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS iii–vii (1973) [hereinafter U.S. DEP'T HEW].

become the cornerstone of the new privacy and "the closest thing the world has to a universal privacy touchstone."[69] Two of the principles reflect data management.[70] The first urges mechanisms "for an individual to prevent information about him obtained for one purpose from being used . . . for other purposes without his consent."[71] The other principle would allow "an individual to correct or amend a record of identifiable information."[72] These two principles empower individuals to manage personal data collected about them. They go well beyond prohibiting the collection or sharing of information—well beyond intrusions. Thus, as a cornerstone of privacy, the fair information practices embody many observers' views of privacy as having a larger legal role in promoting data management interests.[73]

Anti-intrusion and data management are embedded in the first federal law to regulate business use of personal information, the Fair Credit Reporting Act (FCRA) of 1970.[74] That Act targeted one of the industries subject to the most scathing coverage in *The Naked Society*: credit bureaus. Congress strove to meet "the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[75] To prevent intrusions, the FCRA restricted access to credit reports, except for actors with a "permissible purpose," such as landlords, lenders, and insurers.[76] On the data management side, the FCRA provided consumers with the right to have copies of their files and to dispute inaccuracies.[77] A related combination of first-person

---

69 Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 954, 959 (2017).

70 Some of those principles reflect anti-intrusion. Most directly, organizations should not disclose collected information to third parties without legal authorization or consent of the individual. U.S. DEP'T HEW, *supra* note 68, at 41.

71 *Id.*

72 *Id.*

73 *See, e.g.*, Schwartz, *supra* note 27 and accompanying text (providing examples of this view).

74 15 U.S.C. § 1681. Other earlier acts constrained private actors in different ways, such as The Wiretap Act of 1968. 18 U.S.C. § 2510–2522 (constraining nonconsensual interception of electronic and other communications).

75 15 U.S.C. § 1681(b).

76 15 U.S.C. § 1681b The FCRA also gives users control over whether any access is possible by requiring credit bureaus to allow consumers to freeze their credit reports. 15 U.S.C. § 1681c-1(i).

77 15 U.S.C. § 1681g.

access rights and third-party transfer restrictions characterizes two statutes enacted in 1974: the Privacy Act, which applied only to federal agency information about individuals,[78] and the Family Educational Rights and Privacy Act.[79]

Following this wave of privacy legislation, Congress largely ignored the topic for a decade. When lawmakers returned to the subject, they took a strong turn toward anti-intrusion. In 1986, after President Ronald Reagan became concerned about hackers,[80] lawmakers enacted the CFAA to provide for criminal prosecution of anyone who used computers with "unauthorized access."[81] The Act would later become one of the most powerful privacy pretext statutes.[82]

Several other statutes in the 1980s and 1990s emphasized anti-intrusion, targeting everything from unwanted telephone calls[83] to disclosure of video rental history.[84] This emphasis reflected the growing realization that networked computers made people susceptible to intrusions.[85]

The most notable exception to those anti-intrusion statutes was HIPAA, passed in 1996.[86] Lawmakers' primary goal was to promote third-party access to private medical records by facilitating the "efficient" electronic exchange of health care information among hospitals, insurers, and other medical industry actors.[87] To do so, HIPPA imposed common database standards and required medical actors to transfer records to other actors.[88] That data portability was intended to empower individual patients with greater choice of providers and a better chance at life-saving care, while also in theory

---

78 5 U.S.C. § 552a.

79 20 U.S.C. § 1232g.

80 Fred Kaplan, *WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES (Feb. 19, 2016), https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html [https://perma.cc/MT94-BE9E].

81 18 U.S.C. § 1030.

82 *See infra* subpart II.A.

83 Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227.

84 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710; *see also* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

85 *See* Kaplan, *supra* note 80.

86 Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936, sec. 261 (codified as amended at 42 U.S.C. § 1320d note).

87 *See* 42 U.S.C. § 1320d-2.

88 *Id.*

saving the medical system billions of dollars.[89]

Instead, HIPAA is a case study in how anti-intrusion norms can swallow data management norms. Although the primary goal of HIPAA was improving data management, Congress recognized that the increased transfer and centralization of information raised the risk of harmful disclosures and misuse. For that reason, the statute required the Department of Health and Human Services to issue rules promoting privacy and protection of health data.[90] Those rules later provided patients with the right to notice, security, and consent for many third-party disclosures.[91] The agency framed those rules in the context of the Fourth Amendment, the Declaration of Independence, and fundamental rights.[92]

In the ensuing years, health providers routinely cited HIPAA in resisting sharing medical information with other health providers.[93] Consequently, in both impact and perception, anti-intrusion has become the face of what started as one of the most important data management statutes. That migration has become a blueprint for privacy pretexts in the information age.[94]

The judicial approach to privacy demonstrates an even greater focus on anti-intrusion than do statutes. In 1976, the Supreme Court extended substantive due process protections to information. In *Whalen v. Roe*, the Court declared that the Constitution established a "zone of privacy" that protected "the individual interest in avoiding disclosure of personal matters."[95] In its conceptualization of privacy, the Court did not include the data management principles beginning to emerge at the time. Subsequent judicial opinions have routinely linked privacy to the anti-intrusion image of an

---

89 *See* Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 113, 116 (2008).

90 *See* HIPAA, sec. 1128C(a)(3)(ii), 45 C.F.R. § 164.524 (2022).

91 *See, e.g.*, 45 C.F.R. § 164.502 (2020) (detailing such patient protections). The rules also provided patients with the right to inspect their files to ensure accuracy, which is more of a data management impulse. *Id.*

92 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462, 82463–64 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

93 *See* Jessica Jardine Wilkes, *The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care*, 2014 BYU L. REV. 1213, 1241; Carleen M. Zubrzycki, *Privacy from Doctors*, 39 YALE L. & POL'Y REV. 526, 533 (2021).

94 *See infra* subpart III.A.

95 429 U.S. 589, 598–99 (1977) (finding that there had not been an unconstitutional intrusion of privacy).

overbearing Orwellian government spying on us.[96]

Over the past two decades, there have been some signs of the potential for data management to emerge from the shadows of anti-intrusion. Speaking about privacy in Congress in 2006, Representative Ted Strickland declared that the "patient does not want to be 'left alone' in the treatment relationship . . . . Today, good health care requires that the professional's findings be entered into a permanent health care record that is available to multiple other parties."[97] New legal rules under the Obama and Trump administrations accordingly pushed the access side of medical records forward.[98]

The ubiquity and importance of networked digital technologies has further helped elevate data management in the 2010s. The Dodd-Frank Act of 2010 required financial institutions to share consumers' data upon request in electronic format, subject to Consumer Financial Protection Bureau (CFPB) rulemaking.[99] The General Data Protection Regulation (GDPR) in 2016 and the California Consumer Privacy Act of 2020 empowered consumers both to access information that companies maintain on them and to share it with third parties.[100]

Despite these recent advances for data management, courts and federal lawmakers have continued to focus their privacy attention mostly on anti-intrusion.[101] In 2021, the Supreme Court evinced a heightened degree of hostility to data management legislation. In *TransUnion LLC v. Ramirez*, class action plaintiffs brought suit under the Fair Credit Reporting

---

96 *See* Margaret Hu, *Orwell's* 1984 *and Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1832–33, 1873 (2017) (surveying judicial references to Orwell's *1984* and analogies to "Big Brother").

97 152 Cong. Rec. E 719 (May 3, 2006) (statement of Hon. Ted Strickland of Ohio). Some courts have, however, taken a broader approach to applying *Whalen*'s interest in decision-making independence. *See* Schwartz, *supra* note 27, at 581–82.

98 45 C.F.R. §§ 171.100–.303 (2020). This rule was authorized under the 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016) (codified as amended in scatter sections of 42 U.S.C.).

99 Dodd-Frank Wall Street Reform and Consumer Protection Act § 1033(a), 12 U.S.C. § 5533(a).

100 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 15, 20, 2016 O.J. (L 119) 38 (EU); CAL. CIV. CODE § 1798.100 (West 2018).

101 *See, e.g.*, Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1270 (2018) ("Courts and lawmakers keep defining privacy in narrow ways, such as secrecy, ignoring privacy in social contexts and new potential misuses of privacy information.").

Act of 1970 against TransUnion[102] for labeling the plaintiffs as potential terrorists after scanning the Do-Not-Fly list and finding that their names matched.[103] The company took no other action to verify that the two people were the same.[104] The plaintiffs argued that the credit reporting agency had not followed reasonable procedures to ensure the accuracy of its files as required under the FCRA.[105] The FCRA granted individuals a right to view all information in their file, and provided them with a private right of action to enforce that right.[106]

The Court essentially invalidated that data management right of action.[107] It held that most of the class action members lacked standing because there was no concrete harm: TransUnion had not yet provided their credit reports to third parties.[108] TransUnion had not shared that information in an unwanted way. It merely inaccurately labeled those plaintiffs in its internal files.[109] The FCRA's philosophy that individuals have a right to manage data about them before that data is accessed by a third party seemed to be a foreign concept to the Court. Rather than embracing data management norms, the Court hewed closer to the common law notion of an intrusion, in this case the unwanted transfer of information, before holding the credit reporting agency accountable.[110]

B. Unifying Themes

This legal background is helpful context for analyzing privacy pretexts. As Julie Cohen and James Boyle have emphasized, in analyzing the information economy, it is a mistake to ask only how the law should change in response. We must also recognize how the private sector mobilizes the law.[111] Yet seeing how that mobilization unfolds requires paying "more attention to the legal forms in which information

---

102 141 S. Ct. 2190, 2190 (2021).

103 *Id.* at 2201.

104 *Id.*

105 *Id.* at 2208.

106 *Id.* at 2200–01.

107 *Id.* at 2209–13.

108 *Id.* at 2212.

109 *Id.* at 2210.

110 *Id.* ("The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."). For a more extended discussion of some of these issues prior to *TransUnion*, see Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022); COHEN, *supra* note 5, at 150–51.

111 *See* BOYLE, *supra* note 44, at 12; Cohen, *supra* note 44.

issues are framed, debated, and resolved."[112] The above sketch of information privacy's origins demonstrates three themes about privacy legal forms that will run throughout the rest of the Article: salience, economics, and access.

First, there is a salience asymmetry between anti-intrusion and data management. When legislation began with data management goals—most notably, with credit reporting and health care—Congress rightly felt compelled to also address anti-intrusion issues.[113] Conversely, when intrusions motivated legislation, as with the CFAA, Congress did not consider the corresponding data management implications. This contrast helps demonstrate the supremacy of anti-intrusion norms over data management norms. Intrusion has a much older lineage. Its deep roots can be seen in the common law and the Constitution. By the time today's largest platforms emerged—and by the time personal data became big business in many other industries, such as consumer finance—the anti-intrusion principle dominated statutory and judicial conceptions of privacy.

Second, from a policy perspective, data management has a much stronger normative grounding in economics than does anti-intrusion. Whereas individual rights tend to justify anti-intrusion laws, economic theory provides one of the strongest rationales for data management laws, such as HIPAA.[114] To be clear, data management can also be justified from a rights perspective—the right to be free of inaccuracies or to access data about oneself, for instance. However, data accuracy and access are also essential for functioning markets. In practice, data management restrictions on businesses are heavily influenced by economic concerns, such as making financial markets function more effectively through better credit data or lower health care costs. When anti-intrusion restrictions are imposed on business activity, they are more likely to be seen as in tension with economic interests.

Finally, the notion of access has shifted and expanded as privacy has developed. Anti-intrusion is mostly oriented around limiting access to information. However, as the field evolved to incorporate data management principles, laws such as HIPAA showed how at least some mandated third-party access is important for comprehensive privacy legislation.

These themes do not mean that anti-intrusion is inevitably

---

112 BOYLE, *supra* note 44, at 12.

113 *Cf.* Hartzog & Richards, *supra* note 40, at 1704.

114 *See supra* note 86 and accompanying text.

in opposition to data management.[115] Instead, these tensions surrounding salience, economics, and access are noteworthy because they create openings for businesses to opportunistically deploy privacy in harmful ways.

II
REPURPOSING PRIVACY

Businesses use privacy pretexts in two main contexts. First, they cite privacy to withhold information from private actors, both competitors and digital helpers. Second, they limit regulatory information sought by administrative agencies and other actors, such as academic researchers and journalists, who might use information to promote accountability. This Part surveys efforts in each of these areas. Later sections will elaborate on why this third-party access to market and regulatory information is important to markets and society.[116]

A. Blocking Market Information

Many large companies have cited privacy as a reason not to share data with private entities. These companies include large tech platforms such as Meta (Facebook), Alphabet (Google), and Apple, as well as large banks such as Bank of America and Capital One. In each of these instances, the lack of data has the potential to weaken markets, whether by cutting off data from competitors or digital helpers.

1. *Keeping Information from Competitors*

Facebook provides an informative case study of cutting off information from competitors. Thousands of pages of leaked emails and other internal documents illuminate Facebook executives' motives.[117] The social network's leadership systematically monitored which apps were both (1) growing in popularity and (2) offering competing services. Facebook then restricted such apps' access to data.[118] These apps include LinkedIn, a competing social network; Pinterest, which competes with Facebook-owned Instagram; and MessageMe, which offers messaging services like Facebook's WhatsApp.[119]

---

115 The degree of harmony varies by context, but they are overall compatible. *See infra* Part IV.

116 *See infra* subpart III.B.

117 *See Facebook Leaked Documents*, *supra* note 1.

118 *See id.* at 1029.

119 *See id.* In some cases, the only way that the apps could retain access to the Facebook platform was to share with Facebook all of their social data—their

The leaked emails also expose how Facebook sought to frame the withholding of information as helping to protect users' privacy.[120] One vice-president explained that "the messaging to the ecosystem becomes that we are deprecating a few things for privacy reasons."[121] Another internal slide deck described the removal of third-party access to data about users' friends as a "[b]ig potential privacy win" while acknowledging that the real impact was "mostly moot" because favored partners could get that same access through Facebook in other ways.[122] These justifications reflect the anti-intrusion face of privacy because they are rooted in limiting third-party access to Facebook's data.

Despite Facebook's external privacy justifications, the emails show that the company was selectively targeting access restrictions at the fastest-growing rival apps it viewed as posing a "competitive threat."[123] Moreover, around the time that Facebook restricted data access to competitors, it expanded data access to heavy advertisers that were not competitors, like Amazon and Netflix.[124] Facebook's emails and internal documents therefore indicate that privacy concerns were a façade to cover Facebook's real motivations for cutting off data: to hobble potential competitors.

Apple offers a contrast to the example of Facebook, both in the difficulty in characterizing the pretext and the nature of the restriction. Unlike Facebook's targeted restrictions, Apple created access barriers to all third-party apps. It cited customers' privacy interests in not having third-party apps track them and collect excess data.[125] For instance, the app developer Tile helps people locate their lost items.[126] Following the changes, Apple made the Tile app obtain user permission

---

most valuable assets. Complaint ¶ 12, Reveal Chat Holdco LLC, v. Facebook, Inc., 471 F. Supp. 3d 981 (N.D. Cal. 2020) (No. 3:20-cv-363), 2020 WL 256483.

120 *See, e.g.*, *Facebook Leaked Documents*, *supra* note 1, at 462–63 (explaining how Facebook would say policies were "for privacy reasons . . . while not necessarily being the most privacy sensitive.").

121 *See id.* at 740.

122 *See id.* at 777.

123 *See id.* at 1029, 1033 (targeting also those "present[ing] a significant overlap with our product roadmap").

124 *Id.* at 359, 575, 1311. Note that in areas where Facebook viewed Amazon as a competitor, the social network limited access. *See id.* at 360.

125 Apple, *Privacy: App Tracking Transparency*, YOUTUBE, at 00:30 (Apr. 26, 2021), https://www.youtube.com/watch?v=Ihw_Al4RNno [https://perma.cc/XV77-SJH2] ("[S]ome apps have trackers embedded in them that are taking more data than they need.").

126 *Privacy Policy*, TILE, https://www.thetileapp.com/privacy [https://perma.cc/H9TJ-CHU2] (last visited, Dec. 12, 2021).

for "tracking" before turning location data on.[127] Without location data, the app cannot offer its core services.

That change sounds reasonable, and like Facebook's moves, it may overall advance at least some privacy interests. Apple's motives become murkier, however, when considering that Apple did not provide similar tracking and data collection protections with respect to its own apps. For instance, Apple's app Find My, like Tile, helps people to locate items. Yet Find My, unlike Tile, defaulted to location tracking "on" even after Apple announced its universal new "protections" against tracking.[128] That subtle difference matters enormously because consumers overwhelmingly tend to stick with defaults; 94% of Apple customers stayed with the default of declining data collection when prompted to choose.[129] Without a trove of leaked internal documents, it is more difficult to assess Apple's motivations. Nonetheless, the fact that Apple did not believe an extra layer of warning was necessary for consumers using its own comparable device tracking app, and the fact that the move helps Apple to limit apps competing with its own, suggest that the company was using privacy as an anticompetitive pretext.[130]

Privacy pretexts are not limited to the app ecosystem. Amazon engages in similar rhetoric with third-party manufacturers. In one instance, the smart-speaker company Sonos requested anonymized error rate data for when consumers used the company's speakers with Amazon's digital voice assistant, Alexa.[131] Sonos wanted that data to improve the quality of its speakers' responses to voice commands.[132] Amazon cited privacy as the reason for declining the request.[133] Yet it offered no law in support of that assertion because there was no strong candidate.

---

127 *See id.*

128 H.R. COMM. ON THE JUDICIARY, SUBCOMM. ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REP. AND RECOMMENDATIONS 55 (2020), https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf [https://perma.cc/3QRL-2N4D].

129 *See* Greg Bensinger, *Americans Actually Want Privacy. Shocking.*, N.Y. TIMES (May 20, 2021), https://www.nytimes.com/2021/05/20/opinion/apple-facebook-ios-privacy.html [https://perma.cc/KNF6-SEW8].

130 For a helpful summary of the anticompetitive nature of Apple's actions, ironically funded by Facebook, see Sokol & Zhu, *supra* note 7.

131 Written Testimony of Eddie Lazarus Before Subcomm. on Competition Pol'y, Antitrust, & Consumer Rts. of the S. Comm. on the Judiciary, 117th Cong. 6 (June 15, 2021).

132 *Id.*

133 *Id.* at 6–7.

An alternative explanation is that Amazon withheld the anonymized error data to give Amazon's own smart speaker devices a competitive advantage through better access to product quality information. After all, Amazon itself recorded people's conversations in their homes without users' permission or even awareness.[134] Moreover, Amazon shared actual recordings of consumers' in-home conversations with independent consultants it had hired—thereby handing over much more sensitive data to third parties than what Sonos requested.[135] Amazon's broader behavior with respect to data thus suggests Amazon may have been using privacy as a pretext to keep anonymized voice data from Sonos.[136]

As a final example, Google abruptly stopped providing advertisers with access even to users' anonymized and encrypted ID data, citing privacy.[137] As a result, advertisers had to depend on Google for analyzing the success of their Google advertising, and they were required to pay a fee for those analytics.[138] No longer could advertisers go to third-party analytics firms to determine which advertising was most successful. Tellingly, after advertisers paid for Google's extra service, they could once again access encrypted user IDs.[139] Google also purchased transaction data from MasterCard and other financial institutions, which it used to match in-store purchases with Google advertising, and then shared those insights with advertisers.[140] These accompanying activities suggest that, despite its claims, Google was not driven to block

---

134 *Id.*

135 *Id.*

136 Additionally, this is one example of Amazon's broader competitive strategy to systematically block others from accessing its data while simultaneously collecting sensitive data from third-parties, including small businesses selling on its marketplace. Amazon studies which third-party products are successful, and then copies them, helped by its vast resources and control over the marketplace searches. *See* Dana Mattioli, *Amazon Scooped Up Data from Its Own Sellers to Launch Competing Products*, WALL ST. J. (Apr. 23, 2020), https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015 [https://perma.cc/3XTR-HXNL].

137 *See* Complaint ¶ 140, Texas v. Google LLC, No. 4:20-cv-00957 (E.D. Tex. Dec. 16, 2020).

138 *Id.*

139 *Id.*; *see also* Dina Srinivasan, *Why Google Dominates Advertising Markets: Competition Policy Should Lean on the Principles of Financial Market Regulation*, 24 STAN. TECH. L. REV. 55, 102–06 (2020).

140 Mark Bergen & Jennifer Surane, *Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales*, BLOOMBERG (Aug. 31, 2018), https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales [https://perma.cc/Z5FX-BH6X].

access because of some overriding desire to protect people from having their information transferred to third parties.

Business use of privacy to block competitor access is not limited to the examples in this section. Other online platforms, such as LinkedIn, have cited privacy to justify blocking startups from data that the platforms themselves sell to others.[141] Many other platforms, including Twitter, sell access to user data, as do data brokers.[142] Moreover, some of the pretexts discussed in the following section on digital helpers, like those used by financial institutions, also undermine businesses with some competing product overlap. These examples suggest that online platforms widely use privacy as a justification for blocking competitors from accessing information. As more industries monetize data, and thereby overlap more with one another, these pretexts have the potential to expand even further.

The examples in this section share some common features that can begin to help to identify privacy pretexts. The business asserting privacy often engages in inconsistent behavior, such as not subjecting their own collection of data to the same protections they are imposing on others (Apple) or selling the same access that they are claiming to block in the name of privacy (Facebook). Additionally, privacy pretexts allow some monetary gain—beyond consumer good will—to the incumbent from asserting the privacy interest. Finally, and most importantly, each example raises the possibility of harming markets by weakening competition. Related themes can be seen in the following sections.

2. *Keeping Information from Digital Helpers*

Incumbents employ privacy pretexts not only to keep information from direct competitors but also to undermine third parties that consumers *choose* to use for help in dealing with the incumbents. This behavior is concerning because digital helpers can improve consumer welfare by lowering prices, adding convenience, and giving consumers greater choice.[143] For instance, Expedia makes it easier to search

---

141 HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 994–95 (9th Cir. 2019).

142 *See* Erin Bernstein & Theresa J. Lee, *Where the Consumer Is the Commodity: The Difficulty with the Current Definition of Commercial Speech*, 2013 MICH. ST. L. REV. 39, 62; Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. 1184, 1219 (2022).

143 This effect is in addition to any improvements provided by directly competing with the incumbents, and some digital helpers do both advising and competing. *See generally* Van Loo, *Digital Market Perfection*, *supra* note 7, at 830–

among airlines for the best flight, while mortgage calculators help home buyers find the lowest interest rate.[144] Companies use two main avenues to block information from digital helpers: institutional and legal.

a. *Institutional Mechanisms for Blocking Information from Private Actors*

A company can use its relationship with customers to limit third-party information access. The most powerful relational mechanism for control is the customer account. A case study comes from finance. A new generation of financial technology companies ("fintechs"), like Mint, NerdWallet, and Credit Karma, originally sought to democratize financial savvy by advising consumers how best to save, invest, and borrow. For these digital assistants to be most helpful, they need details about the individual's financial profile, much of which is most readily available in the customer's existing financial accounts.[145] Personal data is necessary for providing consumer financial advice because credit products are priced based on factors like income and non-payment risk. Yet it is prohibitively time-intensive for individuals to go to each bank's website, enter their personal information, and get a quote. That is one reason why approximately half of all home buyers get only one quote on their mortgage, often costing them tens of thousands of dollars in higher interest rates over the course of the loan.[146] Consumers decide to share personal financial information with fintechs largely with the goal of saving money.[147]

Given these intermediaries' potential to help consumers find lower prices, it is unsurprising that incumbent financial institutions have resisted them. Banks sell a large array of consumer financial products beyond checking accounts, such as credit cards and loans. Banks thus prefer that the customer look to them for all products, rather than allowing fintechs to help consumers shop around.

Consequently, in fintechs' early days, at a critical time when they could have rapidly attracted a large base of

---

33 (discussing promise and risks of empowering digital intermediaries like Expedia).

144 *See, e.g.*, *id.* at 835–36 (describing AI's potential to expedite mortgage application processes).

145 *See* Van Loo, *Making Innovation More Competitive*, *supra* note 7, at 240.

146 *See* Richard Cordray, *Foreword: Consumer Protection in the Financial Marketplace*, 9 HARV. L. & POL'Y REV. 307, 323 (2015).

147 *See id.*

customers, Bank of America, Capital One, and other incumbents technologically blocked fintechs from accessing customer accounts, despite customers granting access.[148] Banks justified the move with anti-intrusion norms, citing security concerns.[149] These barriers matter even if banks could not outright block fintechs permanently due to regulatory pressure and customer demand.[150] Even temporary blocking of a fintech's access can cause consumers to be frustrated with the fintech during a crucial early period of adoption. Many fintechs have had to either strike agreements with banks or continually update their systems to work around barriers banks create, thereby raising costs or making them dependent on banks for seamless access.[151]

Banks also tried another approach to gain control: direct communications to consumers. For example, Bank of America sent out an email titled "Important information about using third-party apps and websites."[152] The email told consumers that "[s]haring your login information can be risky" and went on to summarize those risks, which include the possibility that the login information given to the third party would be compromised.[153] Instead, Bank of America encouraged consumers to use the third-party app through their Security Center.[154] When consumers agree to do so, they are giving Bank of America additional power over the third-party tool, making it less likely that the tool can offer services that the bank dislikes.

These dynamics may explain why most fintechs rapidly moved away from their founding goals of advising consumers

---

148 Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1286 (2017) [hereinafter Van Loo, *Rise of the Digital Regulator*] (discussing this strategy).

149 *See* Nathan DiCamillo, *Capital One Mends Fences with One Aggregator, Deepens Relationship with Another*, AM. BANKER (Aug. 10, 2018), https://www.nationalmortgagenews.com/news/capital-one-mends-fences-with-aggregators-opens-access-to-data?brief=00000158-07c7-d3f4-a9f9-37df9bc10000 [https://perma.cc/4GFY-5L42]; Memorandum from Rebecca Heironimus, Managing Vice President, Capital One Fin. Corp., to the Consumer Fin. Protection Bureau 5, 10 (Feb. 18, 2020). Data aggregators now play a central role in this issue of sharing data. *See* Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 UTAH L. REV. 1277, 1331.

150 *See, e.g.*, *infra* note 173 and accompanying text (discussing the CFPB's issuance of guidance).

151 *See id.*

152 *See* E-mail from Bank of America Customer Service, customerservice@emcom.bankofamerica.com, on Important Information About Using Third-Party Apps and Websites, (Apr. 13, 2021) (on file with author)..

153 *Id.*

154 *Id.*

on the best market choices.[155] Instead, they began emphasizing other forms of advice that would not direct business away from banks, such as how much to save rather than invest. By controlling account access, banks force fintechs to be careful about offering any product that might threaten banks' interests in retaining customers. Customer use of the Security Center would give Bank of America control over which third-party apps obtain access and what information the apps can see. That control thus enables Bank of America to influence data flows for its profits at the expense of data management.

To be clear, protecting privacy in financial information is important. Financial data is among the most sensitive types of information, and "[i]f an individual's financial information is placed in the wrong hands, it can have significant consequences."[156] However, banks did not calibrate their response to focus on security and allow full fintech access upon request by the customer. Instead, they proceeded in a manner that maximized bank control and obstruction of third parties. Additionally, it is debatable whether a bank's decades-old security system is superior to that of a technology company that built its systems only a few years ago, especially since banks typically build newer features onto their clunky legacy information systems.[157]

Either way, banks' declarations of privacy motivations are inconsistent with how they collect large amounts of customer information while transferring that data to affiliates and insufficiently investing in data security.[158] Their information-blocking actions are more consistent with banks' widespread fear that fintech startups will disrupt the industry's high profit margins, which are boosted by limited consumer information and rationality.[159] By hindering fintechs, banks have helped not only to limit consumers' product choices but also to keep consumers without powerful financial advisors to decide among existing choices.

---

155 *See* Van Loo, *Digital Market Perfection*, *supra* note 7.

156 Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1125, 1155 (2015).

157 *See* Penny Crosman, *Is Finra's Dire Warning About Data Aggregators on Target?*, AM. BANKER, (Apr. 9, 2018), https://www.americanbanker.com/news/is-finras-dire-warning-about-data-aggregators-on-target [https://perma.cc/9QVK-CBJC].

158 *See id.*

159 *See* Van Loo, *Making Innovation More Competitive*, *supra* note 7, at 238–41.

b. *Legal Mechanisms for Blocking Information from Private Actors*

So far in Part I, the privacy pretext examples have been rhetorical. The pretexts were communicated to customers, competitors, or the public. Although the communications were presumably also made with an eye toward future lawsuits or regulatory action, as demonstrated by Facebook's internal emails,[160] they were not immediately legal arguments. Companies can also directly apply pretexts to the law, either by repurposing existing privacy laws or by influencing the shape of new legal rules.

The CFAA provides an example of repurposing an existing law. Various incumbents have used this antihacking statute to block other digital tools from accessing even information readily available on the internet.[161] Consider Power Ventures, which in 2008 unveiled a single interface that aggregated multiple social networks.[162] Rather than going to Facebook to get news, users could go to Power.com and aggregate feeds from several different social networks.[163] Users could post on Power Ventures and distribute the message across several networks.[164] These features also provided more control over users' information flows through third-party access.[165]

That kind of interoperability, at a time when Facebook had only a fraction of its current users, might have enabled a less concentrated social media landscape, yet one where the value of being part of a large network was still preserved.[166] But Facebook argued that Power Ventures had engaged in

---

160 *See, e.g.*, Carole Cadwalladr & Duncan Campbell, *Revealed: Facebook's Global Lobbying Against Data Privacy Laws*, GUARDIAN (Mar. 2, 2019), https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment [https://perma.cc/WAJ6-MCP4]..

161 *See supra* note 17 and accompanying text; Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378–81 (2018). For an excellent in-depth discussion of the CFAA from a property rather than a privacy perspective, see Kadri, supra note 7, at 971–72.

162 Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016).

163 *Id.*

164 *Id.* at 1063.

165 *See id.*

166 On the importance of interoperability in social media, see FRANCIS FUKUYAMA ET AL., STAN. CYBER POL'Y CTR., REPORT OF THE WORKING GROUP ON PLATFORM SCALE 26–27 (2020), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/platform_scale_whitepaper_-cpc-pacs.pdf [https://perma.cc/Z3Q9-9MT6]; Kadri, *supra* note 142, at 993.

unauthorized access under the CFAA.[167] The lawsuit, which Facebook won, forced Power Ventures to shut down.[168] The social network has since then continued to use the CFAA to block or limit third-party access.[169]

More recently, Facebook has blocked even web browsers that offered heightened choice and privacy. One example is the Friendly browser, which prevents websites from tracking users and allows users to sort the Facebook news feed chronologically, which poses a threat to Facebook's strategy of only prioritizing news that keeps users engaged.[170] These information-blocking moves seem inconsistent with Facebook's declarations that it protects privacy by providing users "with transparency and control over how their data is used."[171]

Other incumbents, including Amazon, have used the CFAA to block price comparison tools. In one instance, an app called PriceZombie allowed consumers to compare prices across all major retailers, including Amazon.[172] The app also advised consumers on whether to wait to purchase an item.[173] After quickly growing its user base to over 60,000 active users, PriceZombie suddenly found Amazon blocking its information access.[174] Without the ability to collect information from the largest U.S. online marketplace, it rapidly lost customers and folded.[175]

More broadly, lawyers who work with startups have observed an increasing tendency to tie anti-scraping litigation

---

167 *Power Ventures*, 844 F.3d at 1064. Facebook also made a related claim under a similar California law. *See* CAL. PENAL CODE § 502 (West 2020) (making it a crime to access a computer network without permission).

168 *Power Ventures*, 844 F.3d at 1062.

169 *See, e.g.*, Facebook, Inc. v. BrandTotal Ltd., 499 F. Supp. 3d 720 (N.D. Cal. 2020) (allowing Facebook to pursue its CFAA claim based on third-party privacy grounds).

170 *See* Letter from Andrew Crocker & Mitch Stolz, Senior Staff Att'ys, Elec. Frontier Found., to Ms. del Fierro & Mr. Sherman, Facebook (Nov. 20, 2020), https://www.eff.org/document/eff-letter-facebook-re-friendly [https://perma.cc/FK6K-KCNV].

171 *See Small Business: Personalized Ads*, META, https://www.facebook.com/business/small-business/personalized-ads [https://perma.cc/4NSM-QDLK] (last visited July 25, 2021).

172 *PriceZombie Shutting Down End of the Month Because of Amazon. You Might Be Able to Help*, REDDIT (Mar. 16, 2016), https://www.reddit.com/r/PriceZombie/comments/4ar70l/pricezombie_shutting_down_end_of_the_month [https://perma.cc/PGG2-7HR2].

173 *Id.*

174 *Id.*

175 *Id.*

to privacy concerns.[176] It is impossible to know how influential these innovators might have been on platform concentration. However, these user tools have sought to open the social media echo chamber and lower prices of online marketplaces. The resulting lack of alternatives may have deprived people of innovation, choice, and the full benefits of the data economy.

Firms also make legal arguments by shaping rulemaking or enforcement. Tasked by Congress with writing rules for financial information sharing, the CFPB ultimately did what banks had requested: it declined to write a rule forcing banks to share information with consumer-approved digital helpers.[177] Instead, the agency released a set of nonbinding principles for industry to consult.[178] The agency's main reason for declining to write a rule was concern about data security and privacy, as bank lobbyists had stressed.[179]

This outcome is unsatisfactory from a data management perspective because the absence of a clear legal obligation puts legacy financial institutions in a position of informational control over consumer tools. Facing a similar question, the U.K. and other countries have opted to require banks to share information with fintechs.[180]

It is difficult to know the full implications of the misappropriation of the CFAA and broader use of privacy to slow, coopt, or shut down consumer tools. In 2020 and 2021, courts curtailed CFAA abuse and recognized that expansive readings of the CFAA would turn "each website into its own criminal jurisdiction and each webmaster into his own legislature."[181] But other privacy arguments remain, and because of the CFAA, many different businesses and digital

---

176 Benjamin L.W. Sobel, *A New Common Law of Web Scraping*, 25 LEWIS & CLARK L. REV. 147 (2021) (observing that businesses are becoming more skilled at tying anti-scraping arguments to privacy).

177 *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (Oct.18, 2017), https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/ [https://perma.cc/9VJU-JAAU].

178 *Id.*

179 *See id.*

180 *See, e.g.*, COMPETITION AND MKTS. AUTH., RETAIL BANKING MARKET INVESTIGATION 649 (Aug. 9, 2016), https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf [https://perma.cc/LN9T-UG75] (mandating financial interoperability).

181 Sandvig v. Barr, 451 F. Supp. 3d 73, 88 (D.D.C. 2020); *see also* Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021) (limiting CFAA liability to unauthorized access, not authorized access for an improper purpose). The extent to which this ruling will remove the CFAA from privacy pretexts remains unclear.

helpers never had a chance to fully launch during the most attractive early window of growth opportunity for competitors and digital assistants. Some of these could have significantly altered the platform ecosystem at a crucial time in its development. Thus, privacy pretexts' harms to consumers, markets, and innovation are potentially immense.

B. Blocking Regulatory Information

Businesses have attempted to use anti-intrusion norms to fight against a crucial tool for accountability: regulatory information collection. This move targets three main categories of regulatory information. First, for laws that depend on private enforcement, individuals initiating lawsuits require access to information through discovery. Second, administrative agencies, like the FTC and CFPB, rely on either ex post investigations or ongoing monitoring for compliance.[182] Third, independent researchers collect data to identify legal violations, thereby alerting authorities to the need to act.

In the first of these categories, court discovery, individuals trying to enforce their rights have sometimes met an informational wall built on anti-intrusion arguments. In one representative case, class action lawyers sued Joe's Crab Shack, a nationwide restaurant chain, for minimum-wage violations.[183] Joe's Crab Shack tried to prevent the plaintiff from using employee contact information by citing the privacy interests of the employees.[184] The defendants did not mention any specific law, but rather seemed to be appealing to the court's general sense of privacy.[185] As another example, in a securities fraud case, a bank had allegedly dumped "insider" stock, but the bank argued it should not have to provide information about clients "due to privacy considerations."[186] Sometimes defendants cite a specific statute—such as the main consumer financial privacy statute, Gramm-Leach-Bliley—to fight discovery.[187]

---

182 *See* Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 398 (2019) [hereinafter Van Loo, *Regulatory Monitors*].

183 Hart v. Crab Addison, Inc., No. 13-cv-6458 (W.D.N.Y. Oct. 28, 2014).

184 Memorandum of Law in Support of Defendants' Motion to Compel and for a Protective Order at 15, Hart v. Crab Addison, Inc., No. 13-cv-6458 (W.D.N.Y. Nov. 2, 2015), 2015 WL 10435296 (arguing the data "infringes on the privacy" of the listed employees).

185 *See id.*

186 *In re* Cases Relating to First National Bank of Keystone, No. 2:99-cv-0992 (S.D. W. Va. filed Nov. 8, 1999).

187 *See, e.g.*, Union Planters Bank, N.A. v. Gavel, No. Civ.A. 02-1224, 2003

Turning to administrative agencies, businesses have attacked information collection both in a generalized manner and as a matter of law. To illustrate the more generalized manner, consider how bank lobbyists' complaints about data security affected the CFPB in 2017, when President Trump appointed Mick Mulvaney as acting director of the agency. One of Mulvaney's first moves was to freeze all data collection, which reflected banks' complaints about data security.[188] That move impeded the agency's regulatory function because the CFPB must know what happens to individual consumers to determine, for instance, whether they have been subject to discriminatory, unfair, or deceptive lending practices. Given the importance of data collection to the agency, a halt "could ultimately cripple the agency's enforcement function."[189] Mulvaney's motives were suspect because he had previously fought the creation of the CFPB and later publicly stated that it should not exist.[190]

A subsequent Inspector General report revealed that Mulvaney's concerns were exaggerated, and Mulvaney was forced to lift the data collection freeze.[191] Nonetheless, for months, anti-intrusion warnings by industry had succeeded in shutting down an important regulator's ability to represent consumers' informational interests in the financial sector.

The CFPB data freeze is one instance of a larger sphere of industry lobbying. Industry regularly lobbies against new information collection rules by citing privacy concerns. For example, in 2016, the CFPB sought to collect more data to determine whether mortgage lenders were discriminating

---

WL 1193671 (E.D. La. Mar. 12, 2003), *vacated and remanded sub nom.* Union Planters Bank Nat. Ass'n v. Salih, 369 F.3d 457 (5th Cir. 2004) (issuing an injunction barring release of information in response to a subpoena because the release would purportedly violate Gramm-Leach-Bliley).

188 *See* John Heltman, *Warren Grills CFPB Head over Data Collection Freeze*, AM. BANKER (Jan. 8, 2018), https://www.americanbanker.com/news/warren-grills-cfpb-head-over-data-collection-freeze [https://perma.cc/RG43-EXV3].

189 John Heltman, *Is CFPB's Data Freeze About Security or a Political Ploy?*, AM. BANKER (Jan. 10, 2018), https://www.americanbanker.com/news/is-cfpbs-data-freeze-about-security-or-a-political-ploy?brief=00000158-07c7-d3f4-a9f9-37df9bc10000 [https://perma.cc/2TPJ-CF5T].

190 *See* David A. Hyman & William E. Kovacic, *Implementing Privacy Policy: Who Should Do What?*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1117, 1140 (2019).

191 *See* Consumer Fin. Prot. Bureau, Off. of Inspector Gen., Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program, 2018-IT-C-003, 2, 4–5 (Feb. 14, 2018) (finding most of the allegations unfounded, but observing that some employees had left phones and laptops unattended in the CFPB's office, and recommending better CFPB inventory of all of the personal information it collected).

based on race.[192] Industry pushed back on privacy grounds, even though the additional data requested was mostly about the loan characteristics.[193] The personal data points to be collected—age and credit score—would be anonymized and that data could already be purchased anyways.[194]

In addition to those more rhetorical, advocacy-related privacy pretexts, regulators have found their formal requests for information regularly resisted on similar grounds in court. For example, in 2011, the FTC investigated a debt collection firm, West Asset Management, for harassing, threatening, and lying to consumers; targeting the wrong individuals for collection action; and improperly withdrawing funds from its customers' bank accounts without authorization.[195] In an effort to find witnesses and evidence, the FTC sought access to customer files.[196] West Asset Management resisted on privacy grounds, citing the possibility that the FTC might hand over such information to third parties.[197]

Businesses have made similar arguments in FTC investigations ranging from a hospital merger to fraud investigations following Volkswagen's falsifying of air pollution tests.[198] One magazine subscription service that had engaged in abusive and deceptive telemarketing practices fought an

---

192 12 C.F.R. § 1003.1 (2018).

193 Craig Nazzaro, *CFPB Must Address Lenders' HMDA Data Privacy Concerns*, AM. BANKER (July 5, 2016), https://www.americanbanker.com/opinion/cfpb-must-address-lenders-hmda-data-privacy-concerns [https://perma.cc/F4G8-REEQ].

194 *Security and Privacy*, QUICKEN LOANS (Jan. 1, 2021), https://www.quickenloans.com/about/legal/security-privacy [https://perma.cc/L7U5-7TAC]. Of course, the real concern here would be that anonymized data can be de-anonymized.

195 Press Release, FTC, *Leading Debt Collector Agrees to Pay Record $2.8 Million to Settle FTC Charges* (Mar. 16, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/leading-debt-collector-agrees-pay-record-28-million-settle-ftc [https://perma.cc/9WXZ-RL4M].

196 FTC Letter Ruling Affirming Denial of West Asset Mgmt, Inc.'s Petition to Limit Civil Investigative Demand at 3, FTC File No. 0723006 (July 2, 2008).

197 FTC Letter Ruling Denying West Asset Mgmt.'s Petition to Limit Civil Investigative Demand at 2, FTC File No. 0723006 (Apr. 18, 2008) (quoting West Asset Management's petition arguing "the requests require the disclosure of confidential and personally identifiable consumer and client information").

198 *See In re* Civil Investigative Demand, 2016 F.T.C. LEXIS 30, at *13 (F.T.C. Feb. 25, 2016) (resisting a CID on privacy grounds as part of a fraud investigation related to the Volkswagen emissions scandal); Phoebe Putney Health Sys., Inc.'s Petition to Quash or Limit Subpoena and Civil Investigative Demand at 10, *In re* Proposed Acquisition by the Hosp. Auth. of Albany-Dougherty Cnty. of Palmyra Park Med. Ctr., Inc. from Palmyra Park Hosp., Inc., , File No. 111-0067 (F.T.C. filed Feb. 25, 2011) (opposing a CID for parts of a hospital's anonymized patient files to determine information such as prices as part of a merger challenge).

FTC Civil Investigatory Demand issued for customer subscription lists by dubbing itself "essentially the guardian of its customers' and employees' private information."[199]

Other agencies, such as the Department of Labor and CFPB, have faced related resistance to formal information requests of businesses, under statutes such as HIPAA, Gramm-Leach-Bliley Act,[200] and the Family Educational Rights and Privacy Act.[201] These diverse challenges to regulators all rely on norms of anti-intrusion. The intrusion is either the court or regulator obtaining sensitive information, or the possibility that, once collected, that information might be further disclosed. These arguments have typically failed in court due to longstanding precedent for declining to recognize the sensitivity of information as a defense to such regulatory information demands.[202]

However, it is of limited consolation that these privacy pretexts often fail as a matter of law, or only freeze data temporarily. Temporary halts to information collection can still cause harm by burdening and slowing regulators. Regulation works best when information transfers smoothly from industry to agency. Consider how Facebook's annual revenues are over 200 times the FTC's annual funding, and Facebook is only one of many well-resourced companies the

---

199 Petition to Quash Civil Investigative Demand at 4, *In re* Civil Investigative Demand Issued on May 6, 2013, to Countrywide Periodicals, LLC, File No. 123145 (F.T.C filed May 31, 2013).

200 *See* Petition for Writ of Certiorari, Koresko v. Chao, No. 05-1501, 2006 WL 1455400 (U.S. filed Mar. 16, 2006) (outlining an extensive resistance to Department of Labor ERISA request based on the Gramm-Leach-Bliley Act and HIPAA).

201 *See* Respondent's Petition to Set Aside or Modify Civil Investigative Demand at 9–11, Center for Excellence in Higher Education, CFPB No. 2019-MISC-Center for Excellence in Higher Education-0001 (filed May 21, 2019) (resisting a predatory student lending investigation). For other CFPB examples, see United Guaranty's Petition to Modify or Set Aside June 20, 2012 Civil Investigative Demand at 17–18, *In re* Civil Investigative Demand Issued to American International Group, Inc., CFPB No. 2012-MISC-American International Group-0001 (filed Dec. 7, 2012) (challenging the collection of "confidential consumer information" by arguing that the CFPB could, as long as it provided notice, later hand over that information to third parties); Petition to Set Aside or Modify the Bureau's Second Civil Investigative Demand at 40, *In re* Firstsource Advantage, LLC, CFPB No. 2017-MISC-Firstsource Advantage, LLC-0001 (filed Oct. 18, 2017) (relying on general privacy notions).

202 *See, e.g.*, FTC v. Invention Submission Corp., 1991-1 Trade Cas. (CCH) ¶ 69,338, ¶ 65,353, 1991 WL 47104 (D.D.C. 1991), *aff'd*, 965 F.2d 1086, 1089 (D.C. Cir. 1992) (holding that the confidential or sensitive nature of the required materials is not a proper basis for limiting the Commission's information demands).

agency must regulate.[203] Even if the arguments ultimately fail in court, fighting pretexts can still limit the total amount of regulation by diverting scarce resources.

Other targets of privacy pretexts include journalists and academics. Although these groups are not technically regulators, their findings often spur regulatory action, particularly at an agency like the FTC, which does not have regulatory monitoring authority enabling it to routinely collect nonpublic information.[204] Academics and journalists who reveal problematic practices can thus be seen as a valuable part of the privacy regulatory framework.[205]

For this reason, platforms also seek to block nongovernmental accountability projects. For example, in 2020, Facebook sent a cease and desist letter to New York University researchers studying the social network's amplification of misinformation.[206] The letter explained that legal action was possible because the research information collection posed a "privacy threat" to users.[207] Although the social network backed away from a lawsuit, it still ultimately cut off the researchers' access by making a questionable claim that it needed to comply with a privacy settlement it entered into with the FTC.[208]

* * *

The prominence of anti-intrusion privacy norms has

---

203 Leah Nylen, *FTC Suffering a Cash Crunch as it Prepares to Battle Facebook*, POLITICO (Dec. 10, 2020), https://www.politico.com/news/2020/12/10/ftc-cash-facebook-lawsuit-444468 [https://perma.cc/8JCU-EMR3].

204 *See generally* Van Loo, *Regulatory Monitors*, *supra* note 182, at 384–86 (comparing degrees of regulatory monitoring authority among agencies).

205 *Cf.* Cary Coglianese, Richard Zeckhauser & Edward Parson, *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 279, 281–85 (2004) (outlining an array of important informal mechanisms for regulatory information collection).

206 Jeff Horwitz, *Facebook Seeks Shutdown of NYU Research Project into Political Ad Targeting*, WALL ST. J. (Oct. 23, 2020), https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533 [https://perma.cc/X9P7-G62Q].

207 *Id.*

208 The claim is suspect because the FTC settlement agreement was about third-party service providers. *See* Decision and Order at 3–4, *In re* Facebook, Inc., No. 092-3184 (F.T.C. July 27, 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/N5TK-YPRW]; *see also* Letter from Samuel Levine, Acting Director of the Bureau of Consumer Protection, to Mark Zuckerberg, Facebook (Aug. 5, 2021), https://www.ftc.gov/blog-posts/2021/08/letter-acting-director-bureau-consumer-protection-samuel-levine-facebook [https://perma.cc/TAE9-57R8] (publicly rejecting Facebook's reliance on the FTC settlement as justification); Kadri, *supra* note 142, at 1188.

created abundant opportunities for pretextual legal and rhetorical arguments. The full impact cannot be solely measured by what is found in court records. There is reason to think that the threats of costly litigation and accompanying reputational harms have discouraged some academics and journalists from collecting information from businesses.[209] Moreover, much administrative regulation lies in the gray area of enforcement discretion. By providing incumbent businesses with a means of challenging a variety of data collection requests, privacy forces regulators and entrepreneurs into defensive positions. Privacy arguments thus risk having a broad chilling effect that makes it harder for laws, norms, and markets to hold businesses accountable.

III
THE ARCHITECTURE OF PRIVACY PRETEXTS

Each category of pretext—blocking information from competitors, consumer helpers, regulators, and researchers—merits nuanced attention. Nonetheless, they all share a common structure. Each applies norms of anti-intrusion to block data management help from third parties. Each also gains persuasive power from privacy's aversion to economics and third-party access. This Part discusses these features in turn. Recognizing the structure helps not only to identify problematic pretexts, but also to develop prescriptions.

A. Privacy Pretexts as Control

Privacy pretexts function by leveraging anti-intrusion fears to weaken data management. Consumers want help from digital assistants in navigating a complex commercial landscape. Users want choice in social media platforms. Plaintiffs seek access to records providing evidence of injuries caused by businesses. Regulators must inspect the use of data sets to hold companies accountable to the law. Smaller businesses need data to be able to challenge incumbents. In these and related contexts, a focus on optimally managing data to advance the interests of those providing the data would support allowing data transfers. Yet businesses warn of the specter of intrusion to divert attention from the benefits of allowing information flows.

These moves violate the basic data management tenet that

---

209 Brief for Kyratso Karahalios et al. as Amici Curiae Supporting Petitioner at 17, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783), 2020 WL 3966114.

personal data should not be used to harm the subjects of that data. If businesses can harness personal data to cause market failures, they can raise prices, reduce choice, and dampen innovation. Those effects are to the economic detriment of the individuals whose data they collected.

In addition to harming the subjects of data, privacy pretexts implicate more collective data management interests. Those interests emphasize the benefits to society when markets provide information to actors who can best deploy it. This paradigm allows for balancing economic goals with noneconomic values, such as human flourishing and the democratic desire for an informed electorate.

Privacy pretexts harm individual and collective data management interests through a common institutional mechanism: cutting off third-party access. When businesses block a fintech from providing mortgage advice or stopping Power Ventures from allowing individuals to access multiple social media sites in one place, anti-intrusion norms prevent individuals from benefitting from their contributions to the data ecosystem. If a patient is able to access a health file or an employee can collect colleagues' contact information to initiate a class action, individuals are better able to advance their own legal interests with respect to the business. From a collective perspective, by blocking information from consumer tools and competitors, businesses make markets less effective as viewed through both neoclassical and behavioral economics.[210] By blocking tools and market incentives that could help address misinformation and electoral manipulation, privacy pretexts can undermine democracy.[211]

Blocking regulatory information involves the same basic concepts because regulators are third-party actors managing data on behalf of individuals. Proof that telemarketers defrauded people requires the regulatory collection of at least some personal information, such as names and phone numbers.[212] Enforcement of debt collection laws requires regulatory analysis of customer data, such as contact information and the amount of the debt incurred.[213] By invoking anti-intrusion principles, businesses obstruct the flow of information to administrative agencies, researchers,

---

210 These points are expanded upon *infra* section III.B.2.

211 *Cf.* FUKUYAMA ET AL., *supra* note 166, at 34–35 (explaining the value of middleware in diluting the outsized editorial control of large, dominant platforms).

212 *See supra* subpart II.B. (discussing telemarketing privacy pretexts).

213 *Id.* (discussing debt collection privacy pretexts).

and courts. These parties play crucial roles in protecting individuals' interests and promoting general stewardship of information resources. Each major pretext used to block third-party information access undermines either the individualized or collective conception of data management goals.

This misuse of anti-intrusion to block data management depends on the highly localized nature of privacy norms. Helen Nissenbaum's influential work conceives of privacy in terms of "contextual integrity."[214] Under this view, privacy wrongs occur when actors violate the contextual norms for information flows.[215] Different contexts—doctors' offices, banks, and grocery stores—have their own norms about what information is appropriate to be collected from whom, and transferred to whom.[216] Appropriateness varies not only based on the industry—such as health care versus retail shopping—but also on whether the third party receiving the medical records is, say, a surgeon rather than one's employer.[217]

By strategically stressing anti-intrusion in very specific contexts where it benefits them, businesses can block information flow to regulators, researchers, competitors, and digital assistants. Those same businesses can simultaneously encourage information flows in other contexts where profitable, such as their own collection of data from customers, by emphasizing different norms associated with data management. The following sections will show how privacy pathologies facilitate this use of pretexts for contextual control.

B. How Privacy Is Hospitable to Pretexts

The strategy of employing anti-intrusion norms to undercut data management works in part because anti-intrusion norms are more visceral. People inherently grasp the threat of an invader watching them or entering their private space to collect information. Conversely, for data management, the harms inflicted (or opportunities missed) are less instinctually alarming.

This difference in danger salience is material to understanding why an emphasis on anti-intrusion eclipses other issues. But salience is only part of the story. Privacy

---

214 *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004).

215 *See id.* at 151.

216 *See id.* at 138.

217 *See id.* at 153.

pretexts also gain strength from the field's tension with (1) economics and (2) third-party access.

1. *Norms: The Subversion of Economics*

Privacy pretexts exploit the field's tense relationship with economics. When privacy advocates and scholars have proposed regulation, they have consistently faced resistance rooted in economics. Common arguments emphasize the high cost of privacy regulation,[218] deprivation of consumers' free choice,[219] and harm to innovation.[220] As Richard Posner put it, "people should not—on economic grounds, in any event—have a right to conceal material facts about themselves."[221] Privacy scholars have understandably sought to deprioritize economics because, when weighed against efficiency, "privacy comes up the loser."[222]

However, inattention to economic justifications deprives data management of powerful normative foundations. That inattention is most evident in efficiency and, to a lesser extent, distributional justice.[223] Efficiency is the single most persuasive rationale for convincing policy makers to enact new market regulations.[224] By depriving digital helpers of data under the guise of privacy, businesses undermine informed and rational consumer decisions that are necessary for efficient markets.[225] Privacy pretexts further undermine efficiency if they conceal platform moves that build monopoly

---

218 *See* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 640 (2002) (observing that the most common concern expressed by payers and providers over proposed HIPAA privacy rules were the high costs).

219 Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 97 (2013) ("If the analogy between data collection and payment made in a voluntary market exchange is persuasive, then information privacy regulation must be judged in light of the risk that it will disrupt this functioning market.").

220 Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J.L. & TECH. 256, 258–59 (2020).

221 Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399 (1978).

222 *See* Cohen, *supra* note 28, at 1904 ("[W]hen privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser."); *see also* SOLOVE, *supra* note 62, at 76–90, 228.

223 In response to accusations that Julie Cohen has shown how privacy is essential for innovation, to counter charges that privacy is anti-innovation. *See* Cohen, *supra* note 28, at 1906.

224 *See* Jedediah Britton-Purdy, David Singh Grewal, Amy Kapczynski & K. Sabeel Rahman, *Building A Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784, 1789–90 (2020).

225 *See id.*

power.[226] Also, preventing regulators from collecting information deprives regulators of the information they need to address market failures.[227] Thus, there are strong efficiency arguments against privacy pretexts. Yet the scholars who argue for the efficiency benefits of data management focus on areas outside of privacy, like business law and contracts.[228]

Addressing the aforementioned market failures related to consumer decisions and monopoly power can also be viewed through the lens of distributive justice. Both uninformed decisions and monopoly power raise prices, causing potentially substantial regressive transfers of wealth across the economy.[229] Data management principles that empower rational decisions, competition, and regulation can thus lead to substantial progressive redistribution. While the privacy literature generally recognizes economic harms to individuals,[230] it rarely pays sustained attention to population-level distributional effects.[231] Sustained distributive justice arguments focused on data management, in particular, tend to come from scholars who focus on other areas or remain largely disconnected from the privacy

---

226 *See supra* Part II.

227 *See* David E.M. Sappington & Joseph E. Stiglitz, *Information and Regulation*, *in* PUBLIC REGULATION: NEW PERSPECTIVES ON INSTITUTIONS AND POLICIES 3–43 (Elizabeth E. Baily ed., 1987).

228 *See, e.g.*, Bar-Gill & Stone, *supra* note 33, at 454–55 (proposing machine-readable data sharing mandates to address consumer market pricing failures); Van Loo, *Digital Market Perfection*, *supra* note 7 (explaining the economic potential for digital assistants that have access to data).

229 *See* Bar-Grill & Stone, *supra* note 33, at 453–54 (explaining how carriers' strategic pricing potentially results in a potentially regressive $13.35 billion annual reduction in consumer surplus); Rory Van Loo, *Broadening Consumer Law: Competition, Protection, and Distribution*, 95 NOTRE DAME L. REV. 211 (2019) [hereinafter Van Loo, *Broadening Consumer Law*] (arguing that higher prices associated with consumer market failures have potentially significant regressive effects that could be ameliorated with information-forcing regulation); Einer Elhauge, *Horizontal Shareholding*, 129 HARV. L. REV. 1267, 1316–17 (2016) (concluding that anticompetitive conduct increases economic inequality).

230 *See, e.g.*, Citron & Solove, *supra* note 110, at 21–22 (arguing that collective privacy harms are often ignored because they do lack the individualistic focus courts associates with cognizable harm).

231 *Cf.* Sara S. Greene, *Stealing (Identity) from the Poor*, 106 MINN. L. REV. 59, 62 (2021) (noting that the raging scholarly debate about data breaches "overlooks those most vulnerable to their consequences: those who are low-income"); Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113, 121 (2011) (showing how the government's supervision of pregnant poor mothers demonstrates that they have fewer privacy rights than other groups); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2010 (2013) ("Policy and academic debates over privacy rules tend not to emphasize the distributive dimensions of those rules . . . .").

literature.[232]

Despite strong economic arguments in favor of data management, privacy scholars have not deployed them in the same way that, say, intellectual property scholars do.[233] Although privacy advocates and scholars have paid some attention to economic *harms* from intrusion, they have underinvested in analyzing economic *gains* from data management.[234]

The limited attention to economic arguments facilitates businesses' ability to deploy self-serving normative hierarchies. One of the strongest arguments used against privacy regulation has drawn on a famous body of privacy research known as the privacy paradox. In actual markets, when consumers are spending real money, they choose functionality, convenience, and low price over privacy.[235] For

---

232 To the extent privacy is mentioned in the sources *supra* note 229, it is to note in passing that the (anti-intrusion) privacy concerns should be addressed. *See, e.g.*, Van Loo, *Broadening Consumer Law*, *supra* note 229, at 253–54 ("The privacy risks must also be weighed should regulators collect consumers' personal data."). Antitrust scholar Nathan Newman has argued that search practices contribute to economic inequality. *See* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 850 (2014). Salomé Viljoena and Julie Cohen have deeply engaged with distributive justice issues, and thereby provided important theoretical and normative foundations, albeit mostly subsumed within larger treatments of collective governance, social inequality, and power. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000) ("Personally-identified data is the wedge that enables 'scientific,' market-driven, and increasingly precise separation of 'haves' from 'have-nots.'"); Viljoen, *supra* note 11, at 586, 642 ("[D]ata relations can materialize unjust group-based relations like racism, sexism, and classism.").

233 *See, e.g.*, BOYLE, *supra* note 44, at 12, 35–46 (engaging with information economics and stating that more attention is needed to understand "the complex reciprocal relationship between our current ideas of politics, justice, efficiency, and entitlement"); JAMES BOYLE & JENNIFER JENKINS, INTELLECTUAL PROPERTY: LAW & THE INFORMATION SOCIETY 1 (5th ed. 2021) (explaining how intellectual property, speech, competition and privacy are four categories for information management that are often in tension); *see also* Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 993 (2012) ("Although IP scholars typically reason in the idiom of efficiency, a small but growing number of them have begun to suggest that distributive justice values should also influence information policy.").

234 This is true of privacy beyond economic matters. *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 441 (2016) (concluding that privacy "is too focused on privacy's costs, often to the exclusion of any benefits").

235 *See* Shara Monteleone, *Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation*, 43 SYRACUSE J. INT'L L. & COM. 69, 86–90 (2015). *But see* Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105 (2020) (arguing that the rational choice model does not account for cognitive biases and platform design tricks that influence consumers).

instance, given the choice between making a few dollars or retaining their online browsing history privacy, consumers will choose to hand over their data and take the money.[236] This conduct is seen as paradoxical because people say they value privacy but fail to act accordingly.[237] Opponents of regulation have used that research to argue that costly restrictions on data collection would go against what people most want.[238]

Privacy pretexts deploy an inverse narrative. They argue for prioritizing anti-intrusion over price, choice, and convenience.[239] Consequently, a counterargument to privacy pretexts would be to stress the privacy paradox research suggesting that people value price, choice, and convenience more than anti-intrusion.[240] After all, those are the very interests that privacy pretexts undermine.[241]

However, privacy's normative framework is not well positioned to make that case because privacy scholars—in order to defend against attacks on valuable privacy policies—have needed to argue against the privacy paradox.[242] The limited privacy attention to economic gains means that in policy debates there is less likely to be consideration of the full benefits to data management rules that would disadvantage powerful incumbents.

Privacy pretexts thus help illustrate the downsides of the field's disconnect from economics. Since data management principles have a stronger economic rationale than do anti-intrusion principles, the deprioritization of economics means that privacy's anti-intrusion norms are more developed than its data management norms.

That normative imbalance also allows firms to strategically deploy economic arguments. When they seek to collect and sell data, firms emphasize the economic benefits of allowing such transfers as a reason to ignore the intrusion. Facebook, for instance, has stressed that its access to users' data is

---

236 *See* Spyros Kokolakis, *Privacy Attitudes and Privacy Behavior: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 COMPUT.S & SEC. 122, 122 (2017).

237 *See id.*

238 *See* Eric Goldman, *The Privacy Hoax*, FORBES (Oct. 14, 2002), https://www.forbes.com/forbes/2002/1014/042.html?sh=268831cc2717 [https://perma.cc/3AGN-MDCH].

239 *See supra* Part II.

240 *See* Kokolakis, *supra* note 236.

241 *See supra* subpart II.A.

242 *See, e.g.*, Waldman, *supra* note 235, at 105–07 (using non-economic factors, such as practical hurdles, cognitive biases, and platform design, to argue against the privacy paradox).

crucial for offering its product for free and for helping small businesses thrive.[243] When businesses instead prefer to block the transfer of the data they hold, they omit the economic drawbacks while calling attention to the intrusion, as Facebook did in selectively blocking third-party access.[244] Businesses are thus dominating the economic narratives that can heavily influence what individuals will see as the appropriate norms for flow of information in a particular context.

2. *Institutions: Privacy's Access Paradox*

Privacy has an uneasy relationship with organizations accessing data. Privacy scholars now certainly recognize the importance of at least some third-party access , especially for regulatory purposes.[245] But much of the field's most influential scholarship over the past sixty years was animated by the need to impose restrictions on information dissemination.[246] Privacy scholars have long worried that laws like FOIA that provide transparency—which is a form of access—can be used to erode privacy.[247] One of privacy's pioneers, Ruth Gavison, grouped the constellation of underlying harms by defining privacy as "a concern for limited accessibility."[248] In other words, privacy's normative imbalance helps to obscure the precise set of pro-access interests that businesses also seek to obscure when they use privacy pretexts. Privacy's traditional anti-access emphasis has thus paved a path for privacy pretexts.[249]

Part of the problem is that the importance of access was less prominent in the main contexts in which anti-intrusion

---

243 *See* Dan Levy, *Speaking Up for Small Businesses*, META (Dec. 16, 2020), https://www.facebook.com/business/news/ios-14-apple-privacy-update-impacts-small-business-ads [https://perma.cc/9RQD-B8X4] (emphasizing Facebook's opposition to Apple's new data tracking restrictions on distributive justice grounds).

244 *See supra* subpart II.A.

245 *See, e.g.*, Schwartz, *supra* note 27, at 555 (asserting "the establishment of effective government oversight of data use" as one of the four necessary elements of a data protection framework that approaches privacy as participation). Julie Cohen has more broadly critiqued self-serving moral narratives and other strategies that "tend to reinforce regimes of technical secrecy" and block public access. COHEN, *supra* note 23, at 210–13.

246 *See, e.g.*, WESTIN, *supra* note 7, at 7 (emphasizing privacy as "claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others").

247 *See, e.g.*, SOLOVE, *supra* note 62, at 151 (warning of transparency laws' threats to privacy).

248 *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980).

249 The main exception is in reference to individuals accessing their own data.

norms developed. The individual did not require access to learn that somebody had published sensitive information about her in the newspaper, the main concern motivating *The Right to Privacy*.[250] When access entered the formative privacy conversations of the 1970s, it was a much more straightforward concept. At that time, it mostly meant individuals having access to their files, such as their credit reports.[251] From the perspective of the individual, such mandates are not an intrusion.

Two institutional changes have since occurred that accentuate the tension between access and anti-intrusion: one to the regulatory state and the other to industrial organization. When the Fair Credit Reporting Act was enacted, the CFPB did not yet exist, and the Act's primary enforcer, the FTC, did not monitor credit reporting agencies to ensure compliance.[252] The idea that regulators should have ready access to private businesses' dealings with consumers was not as well established.[253] However, over the course of the twentieth century, regulatory authority to patrol business conduct—through routine environmental inspections, safety audits, and bank examinations—steadily spread throughout much of the administrative state.[254] With the statutory creation of the CFPB in 2010, regulatory monitoring on behalf of consumers first arrived in full force.[255] Regulatory monitoring, and thus third-party access, is essential for the enforcement of data management in an industrial landscape marked by large, complex, and opaque corporations deploying massive data sets.[256]

The second institutional shift is the rising societal centrality of digital assistants. As markets have become more complex and opaque, with myriad product characteristics, multi-dimensional pricing structures, and lengthy contractual terms, consumers have become less able to assess which purchases are most attractive.[257] Consumers' individual access to massive data sets does little without the help of a

---

250 Warren & Brandeis, *supra* note 58, at 195.

251 *See supra* Part I; COHEN, *supra* note 23, at 209.

252 *See* Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1, 84 (2008).

253 *See* Van Loo, *Regulatory Monitors*, *supra* note 182, at 393.

254 *See id.* at 384–92.

255 *Id.* at 394–95.

256 *See* Van Loo, *The Missing Regulatory State*, *supra* note 9, at 1617–22.

257 *See, e.g.*, Alan Schwartz, *Regulating for Rationality*, 67 STAN. L. REV. 1373, 1376 (2015) (explaining the implausibility of consumers making rational decisions when faced with complicated contractual terms).

sophisticated third party, such as a product search engine, that can analyze or organize the information.[258] Similarly, in the context of social media, the user may need an intermediary tool for greater control over the news received and dissemination of content posted.[259] As more of social and commercial life has migrated online, digital assistants have become much more vital to full participation in society. The most effective digital helpers will often need access to personal information held by incumbent businesses.

The arrival of these two institutional changes after the most formative years of privacy, along with decades of focus on anti-intrusion, help explain the field's weak normative development of third-party access benefits. To be clear, some privacy scholars have criticized the field's excessive emphasis on anti-intrusion, and its unrealistic expectation that the individual can take action to redress the harm.[260] Some have also shown that many of the most important data harms are on the societal level, rather than the individual level.[261] However, they have yet to theorize fully the paradox of the anti-intrusion paradigm obscuring the need to protect what are essentially (societally beneficial) third-party intrusions on the business. Indeed, many leading privacy scholars remain uncomfortable with regulatory monitoring as a solution to privacy.[262] In short, the inattention to developing third-party access norms has paved the way for privacy pretexts as a means of walling off data.

To dig a layer deeper into the institutional stratagem, another way of viewing privacy pretexts is as businesses leveraging privacy's anti-access ethos by asserting themselves as individuals' privacy guardians against dangerous third parties. Yet third-party access is only clearly an unwanted intrusion from the perspective of the incumbent businesses,

---

258 *See* Van Loo, *Rise of the Digital Regulator*, *supra* note 148; FUKUYAMA ET AL., *supra* note 166, at 28.

259 *See, e.g.*, FUKUYAMA ET AL., *supra* note 166, at 35 ("[A] middleware system could offer services that many in our society deem to be urgently needed, such as a robust system of fact-checking and hate-speech moderation.").

260 *See, e.g.*, Solove, *supra* note 12, at 1419–30 (proposing a Kafka-based conception of the privacy problem as more about uncontrolled bureaucratic decisions based on digital files about us without our knowledge).

261 *See, e.g.*, COHEN, *supra* note 5, at 139.

262 *See, e.g.*, Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1579 (2019) (favoring private monitoring for privacy reasons). *But see, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 24 (2014) (proposing FTC access to credit report systems).

whose financial interests are advanced by blocking access to competitors, digital helpers, and regulators.[263] The extent of individuals' support for third-party access to their data would vary by context. In the context of consumer helpers, that consent is usually implicit to the extent consumers are choosing to use the third-party tool.[264] And the privacy paradox research suggests that when competitor access would lower prices, most consumers would be supportive of such access.[265] Support for regulatory access to data would surely be more varied, but that access results from using authority granted by elected representatives—thus, at least in theory, it has the democratically imputed consent of the people.[266] Moreover, whereas the role of businesses as privacy guardians may prove valuable when a government entity, such as the FBI, is seeking information to prosecute one of the company's customers,[267] it makes less sense to assert customers' privacy when a government entity is seeking information to prosecute the business. Privacy pretexts thus operate partly by reframing access that the business views as an intrusion instead as an intrusion on the individual's data.

Ironically, although businesses are using privacy norms in these instances, they are emphasizing an older conception of privacy. Theorists who have more recently argued that privacy is important to protect autonomy, human flourishing, and liberal citizenship were not stating that anti-intrusion was the only way to achieve those goals. They recognized that interests outside of privacy were also important to achieve those goals. Moreover, many newer conceptions of privacy are consistent with, if not supportive of, managed third-party access. For instance, Paul Schwartz argued that we should move beyond

---

263 *See supra* Part I.

264 Of course, these third-party tools raise their own issues of consumer protection and true consent, although the incumbent presumably collected the data through a notice and consent regime, and to allow them to do so but not consumer helpers or challengers would be inconsistent. On the challenges of the notice and consent regime, see, for example, Solove, *supra* note 48, at 1880.

265 *See supra* note 232 and accompanying text.

266 This is clearly a complex issue, and if directly polled, consumers would likely give varying degrees of support depending on whether the data were anonymized, which agency was collecting the data, and for what purpose. However, there is no survey consent test for whether each law should be enforced. For instance, surely it would not be a valid defense to racially disparate predatory lending investigations that most of the bank's customers would prefer not to have their data collected.

267 *See, e.g.*, Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 109–10 (2018) (explaining how businesses often protect users' privacy against crime and intelligence agencies).

"privacy as 'informational seclusion'" and instead approach "privacy as participation."[268] Schwartz was focused more on direct, individual participation, but once one recognizes that full participation in the current digital environment will require the help of digital intermediaries and other third parties, businesses' ability to isolate individuals from the help they need to manage their data is inconsistent with viewing privacy as participation.

There is a final irony in incumbent firms using privacy arguments to block third parties. For years, tech companies lobbied against privacy regulation by claiming that doing so would limit users' access to information.[269] Indeed, as the internet's awesome potential became apparent in the late 1990s, unfettered data access was arguably the main pitch by legal scholars, tech companies, and policy makers against regulating privacy in the information age.[270] However, businesses now use privacy pretexts to justify their own private ordering that restricts access to information. By blocking third-party access, businesses are engaging in the very practice, regulating information flows, that they long said was anathema.

* * *

When in tension with privacy, the flow of information was long thought to be an unstoppable force.[271] Instead, incumbent businesses have exploited the data framework's normative and institutional confusion to selectively halt the flow of information. When a business seeks to allow information to flow, it emphasizes institutional trustworthiness and the economic benefits associated with data management principles. When that same business seeks to block information in another context, it emphasizes the need to protect individual autonomy from intrusions by risky third parties. The implicit message is that the incumbent business should be trusted to sort through these difficult tradeoffs on the individual's behalf. With the user retaining control in theory, businesses thereby seize de facto contextual control of data.

IV

---

268 Schwartz, *supra* note 27, at 555.

269 *See Facebook Leaked Documents*, *supra* note 1, at 877–81 (celebrating successful lobbying based on pro-information flow arguments).

270 *See, e.g.*, COHEN, *supra* note 5, at 5–8.

271 WESTIN, *supra* note 7.

NORMATIVE IMPLICATIONS

The above deconstruction identifies a pattern of behavior in which businesses use anti-intrusion norms to weaken data management. The problem is not so much the pretexts themselves but the normative dysfunctions they reveal and the societal harms they advance. This Part moves from analyzing the problem to theorizing solutions. The architecture of the move to repurpose privacy yields insights into a better regulatory blueprint, one with greater promise to accommodate the societal stakes in data.

A. Allied Access

The privacy framework needs a stronger third-party access principle. An emphasis on allied access would aim to preserve beneficial third-party access to people's data, especially for digital assistants, competitors, researchers, and regulators. Such access would be warranted when individuals or their democratic representatives choose it.[272] In other contexts, a competition analysis would need to be deployed to identify allies, but with a more comprehensive sense of the tradeoffs between access and isolation.[273] The case for embracing such an allied access principle could rest on several rationales.

The most straightforward rationale is viewing allied access as necessary to address market failures. Economic theory supports allied access when digital assistants, competitors, and regulators need access to data to address market failures. The economic case for intervention becomes stronger where the market failures also distribute regressively.[274] Aside from the distributive justice concerns, there is reason to believe that extreme inequality dampens economic growth and necessitates tax redistribution, which further distorts markets.[275] Thus, laws preserving allied access have the potential to greatly improve efficiency and strengthen the economy.[276] Also,

---

272 This covers regulators and digital helpers chosen by consumers.

273 *See infra* subpart IV.B. (outlining a broader set of interests that should be mapped in making such decisions); Douglas, *supra* note 7, at 681 (analyzing how to weigh privacy in the competition analysis).

274 *See supra* subpart III.B.

275 *See* Beth Ann Bovino, Gabriel J. Petek & John B. Chambers, STANDARD & POOR'S RATINGS SERVS., HOW INCREASING INCOME INEQUALITY IS DAMPENING U.S. ECONOMIC GROWTH, AND POSSIBLE WAYS TO CHANGE THE TIDE 3 (Aug. 5, 2014); *cf.* Zachary Liscow, Note, *Reducing Inequality on the Cheap: When Legal Rule Design Should Incorporate Equity as Well as Efficiency*, 123 YALE L.J. 2478, 2482 (2014) (showing how some laws may distribute more efficiently than taxes).

276 *Cf. supra* note 229 (outlining the link between market failures, regulation, and inequality).

economic rationale can justify access mandated to advance non-economic interests, such as addressing the negative externalities caused by misinformation. If privacy were to embrace a more comprehensive economic analysis of data sharing, it should contribute to a stronger norm of allied access.

Allied access finds other support in scholars' conceptualizations of the data economy as creating an informational public domain.[277] A public domain implies rights of access that benefit society and human flourishing.[278] Indeed, a public domain lens helps to resolve the potential paradox of privacy law requiring third-party intrusions by regulators, digital assistants, and competitors.[279] If the data belongs to the public, socially beneficial access is not an intrusion.

Allied access has a more complicated normative relationship to a strict propertarian regime. If data is property, individuals should be able to transfer it. Once the transaction is completed, it is not inevitable from a property framework that individuals must retain access rights regarding that transferred property.[280] However, property rights operate within a web of laws restricting what transactions can be entered into, and under what conditions. Those laws form the infrastructure of markets.[281] Some of those laws even make more personal services or body parts inalienable. Many market laws require administrative agency access, and both consumer protection and antitrust laws may mandate access for digital assistants and competitors.[282] Moreover, a

---

277 *See* BOYLE, *supra* note 44, at 183 (arguing for a more expansive conception of the public domain with an emphasis on intellectual property, and warning of various laws that might get in the way); COHEN, *supra* note 5, at 48 (conceiving of the data economy as built on raw material extraction and creating a "*biopolitical public domain*" that is "foreign to privacy and data protection law").

278 For an extended discussion on the need to balance access with limitations on access in light of the "constitutive importance of tinkering for human flourishing," see COHEN, *supra* note 23, at 187–220.

279 *See supra* section III.B.2. (explaining how access could be seen as an intrusion).

280 For helpful discussions of using intellectual property rights as a model for information privacy, see Pamela p, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); *see also* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295–1301 (2000); Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77, 106 (2019).

281 *See* Hanoch Dagan, Avihay Dorfman, Roy Kreitner & Daniel Markovits, *The Law of the Market*, 83 L. & CONTEMP. PROBS. i, ii (2020) ("[M]arkets necessarily depend on well-designed and well-enforced rules of the game: they rely on, and are constituted by, a legal infrastructure.").

282 *See* Van Loo, *Regulatory Monitors*, *supra* note 182, at 384–89; *supra* Part I

fundamental goal of contract and property law is to promote commercial exchanges.[283]

Thus, to the extent a propertarian regime is justified through or respects economic theory, it is at least consistent with, and perhaps lends normative support to, allied access. The "right to repair" movement, which seeks to preserve consumers' ability to choose third-party repairs rather than need to go to the original manufacturer, on products ranging from computers to cars, indicates how property concepts can translate into a movement in support of access.[284]

Finally, in some contexts allied access finds normative support in the proposition that a legal right must have a means to enforce it. Individuals have long faced difficulties enforcing privacy laws in court.[285] The Supreme Court's 2021 *TransUnion* opinion, by forestalling a private right of action for inaccurate credit reports absent an intrusion, means that some data management regulations can only be enforced by a government representative.[286] Thus, third-party access by a regulator is implied by the existence of data management laws that would not otherwise be enforceable.

Laws promoting allied access would come with the risk that institutions may abuse them. Digital assistants and incumbent businesses might exploit the principle to acquire excess data, in the extreme enabling them to gain monopoly power or erode privacy. Business regulators might share information collected with other agencies, like the FBI, and use it against individuals. Overall, allied access thus risks becoming a tool for undoing some of the privacy movement's important progress.

Steps would need to be taken to mitigate these adverse outcomes, including appropriate legal rules overseeing digital helpers and requirements of anonymization.[287] However,

---

& section III.B.3. (explaining how various laws, including Dodd-Frank Act's consumer protection rules, mandate access).

283 *See* DAVID G. EPSTEIN, BRUCE A. MARKELL & LAWRENCE PONOROFF, CASES AND MATERIALS ON CONTRACTS, MAKING AND DOING DEALS 6, 17 (5th ed. 2018).

284 *See, e.g.*, Nicholas A. Mirr, *Defending the Right to Repair: An Argument for Federal Legislation Guaranteeing the Right to Repair*, 105 IOWA L. REV. 2393, 2411 (2020) (referring to the property components).

285 *Cf.* Citron & Solove, *supra* note 110, at 2 ("Countless privacy violations are not remedied or addressed on the grounds that there has been no cognizable harm.").

286 *See supra* Part I.

287 *See, e.g.*, Maurice E. Stucke & Ariel Ezrachi, *How Digitial Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239, 1287 (2017) (emphasizing competition problems, such as collusion); Van Loo, *Digital Market Perfection*, *supra* note 7, at 823 (discussing broader regulatory oversight

several factors limit these risks. With respect to digital assistants and competitors, allied access would mean sharing information that a business already has with another business that the individual has chosen. The total information shared thus does not increase and stays within the universe that the individual has elected to trust. Additionally, it would be inconsistent to allow the individual to choose to share the information with the incumbent firm but not with other firms, especially while allowing the incumbent to share that same information.

The concern about inter-agency regulatory data sharing is understandable, as regulators do sometimes transfer information to other agencies.[288] However, regulators do not have the expertise, resources, and self-interest to monitor for personal violations.[289] The Privacy Act also restricts information sharing among agencies.[290] More importantly, agencies like the FBI can already readily obtain individuals' data held by companies without a warrant, through the Fourth Amendment's third-party doctrine.[291] They do not need a regulatory back door for obtaining private sector data because they have a front door.

It bears emphasis that an allied access principle is both positive and normative. It describes features of existing information privacy legislation, such as HIPAA's allowance of patient data collection for third-party research or the Dodd-Frank Act's mandate that the CFPB consider open banking rules.[292] More subtly, regulators such as the FTC and CFPB are deputizing large firms as privacy enforcers over smaller businesses.[293] For instance, by settlement order

---

of digital intermediaries); Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 360 (2017) (observing the use of anonymization to overcome privacy concerns in the collection of big data). Another tool is to use data silos, particularly for regulators. *See* Shu-Yi Oei & Diane M. Ring, *"Slack" in the Data Age*, 73 ALA. L. REV. 47, 96 (2021).

288 *See, e.g.*, Hyman, *supra* note 190, at 1140–41 (discussing information sharing).

289 Also, the access gained by regulators would be oriented toward investigating businesses, and would thus collect either anonymized data or large data sets.

290 5 U.S.C. § 552a(b) (prohibiting sharing except in enumerated circumstances).

291 *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that Fourth Amendment protections extend to cellphone location data collected by wireless carriers, but reaffirming third-party doctrine in other circumstances).

292 45 C.F.R. § 164.512(i) (2020) (providing an exception for third-party access, most notably for research purposes designed to improve health care); *supra* Part II.

293 *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*,

Facebook must check app developers' privacy practices.[294] In other words, enforcement currently requires large firms to intrude on smaller ones.[295] Finally, allied access captures a broader theme of third-party in many scholarly proposals for improving governance of the data economy.[296]

Although these developments have begun to elevate beneficial third-party access, they are normatively siloed and existing legal rules lack a comprehensive consideration of data management interests. Particularly in light of privacy's normative asymmetries working against data management, a broad-reaching allied access principle could provide valuable foundations for efforts underway to improve the data regulatory framework.

B. Mapping Data Management

Another implication of privacy pretexts is that the law would benefit from a more nuanced and comprehensive mapping of individuals' data management interests and how they relate to anti-intrusion interests. Privacy pretexts thus provide support for privacy scholars' calls for considering a broad set of interests to safeguard,[297] as well as antitrust scholars' calls for paying greater attention to privacy in competition analyses.[298] Yet by deprioritizing economics and

---

106 VA. L. REV. 467, 496–97 (2020) [hereinafter Van Loo, *The New Gatekeepers*].

294 *See* Decision and Order at 3–4, *In re* Facebook, Inc., No. 092-3184 (F.T.C. July 27, 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/N5TK-YPRW].

295 *See* Van Loo, *The New Gatekeepers*, *supra* note 293, at 499.

296 These proposals range from interoperability to regulatory monitoring. *See, e.g.*, FUKUYAMA ET AL., *supra* note 166, at 35 (proposing third-party algorithmic access to combat misinformation in social media); Citron & Pasquale, *supra* note 262, at 24 (proposing FTC access to credit report systems); Yafit Lev-Aretz, *Data Philanthropy*, 70 HASTINGS L.J. 1491, 1491 (2019) ("The data philanthropy exception reinforces the values at the heart of the FIPs, provides guidance in a field that currently operates in a legal vacuum, and introduces the possibility of responsible sharing by and to smaller market participants."); Mary D. Fan, *The Right to Benefit from Big Data as a Public Resource*, 96 N.Y.U. L. REV. 1438, 1438 (2021) (proposing "a model that permits controlled access and the use of big data for public interest purposes"); Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 604 (1998) (proposing interoperability as a response to network effects); Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311 (2015) (explaining how digital intermediaries are important even in retail goods markets); Packin, *supra* note 149 (discussing access rules).

297 *See supra* Part I.

298 For examples of scholars calling for greater attention to the interface between privacy and competition, see Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON. L. REV. 1009, 1010 (2013); Dina Srinivasan, *The Antitrust*

access, the privacy lens has made it overall less likely that anti-intrusion and data management interests are rigorously balanced against one another, particularly in allied access contexts.[299]

The typical privacy contexts analyzed are those that are most problematic from an anti-intrusion perspective: the individual's sharing of data directly with a business, such as a bank or hospital, or that same business then choosing to transfer data for its own gain.[300] That focus means less attention to contexts in which transfers to third parties might bring data management benefits, such as when the individual would want to transfer the information to third parties.[301]

Again, the contextual focus matters partly because of the flipped hierarchy of economic interests. In the contexts that have traditionally been the focus of privacy—such as the consumer sharing information with a business—economic arguments most directly weigh *against* privacy regulation because it would impose costs. Mapping the interests specific to allied access contexts would mean the opposite. In allied access contexts, economic considerations *support* regulation by advancing competition and informed and rational consumers.[302] A clearer and more comprehensive mapping of data management interests would make it harder for businesses to shift the policy focus to the normative hierarchy they prefer.

Another way to think about privacy pretexts is as incumbents narrowing the contextual focus. The main narrowing has been the focus of much of this paper—businesses urging others to look at only anti-intrusion interests rather than *both* anti-intrusion and data management interests. A second type of analytic narrowing comes once the policy lens succeeds in considering data management. If that occurs, incumbents would still prefer to narrow the data management inquiry by excluding economic interests, instead focusing on a subset of data management interests such as accuracy of the data—which would be more likely to mandate an individual right to access rather than

---

Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 BERKELEY BUS. L.J. 39, 88 (2019).

299 *See supra* subpart III.B.

300 These include the economic benefits to the individual of sharing the information, such as a free digital service or greater choice, as well as the lower regulatory costs imposed on the firm.

301 *See supra* section III.B.1.

302 *See supra* section III.B.2.

third-party access. Any inclusion of data management economic interests might make it harder for incumbents to wall off their data, subject to a competition analysis.

Finally, if the data analysis arrives at economic considerations, the ideal for incumbents is still that the analysis remains in a narrower economic frame, such as solely within an antitrust balancing test. Limiting the analysis to antitrust increases the chances that other economic benefits to data sharing are omitted, such as the more consumer-law-related interest in helping consumers to make informed choices—which is benefitted by independent digital helpers having access to data.[303] Thus, to the extent that the policy analysis remains confined to either anti-intrusion, anti-economics, or a narrow competition analysis, it operates in service of incumbents' data control.

One shift that would help to broaden the analytic lens would be to establish a stronger identity for data management. One of the main goals would be to strengthen the norms surrounding data management, so as to make it harder to brush data management aside by emphasizing anti-intrusion. This shift could happen whether data management is viewed as part of privacy or independent of it.

A comprehensive mapping of interests need not pit anti-intrusion against data management, even in allied access contexts. Granted, a more comprehensive consideration of tradeoffs would sometimes highlight tensions in the bundle of anti-intrusion and data management principles. However, giving greater weight to data management does not mean that anti-intrusion becomes commensurately less important. Consumers would still want assurances that their digital assistants are safeguarding their data and not selling it to data brokers, for instance. Indeed, the balance of interests in allied access contexts may sometimes weigh against sharing certain sensitive information.

At a minimum, comprehensiveness seeks to ensure that the policy outcome does not rest solely on interest hierarchies manipulated by businesses. Incumbents would have a harder time simultaneously arguing *for* prioritizing consumers'

---

303 This statement may strike many non-economist lawyers as confusing because antitrust law is so strongly linked to the concept of competition, but as a matter of economics, many other areas of the law also advance competition. For example, consumer laws advance competition by promoting choice. *See, e.g.*, Van Loo, *Digital Market Perfection*, *supra* note 7, at 830–33 (explaining how digital intermediaries can promote "perfect competition" in the broader economic use of the phrase).

economic interests to fight anti-intrusion regulation while arguing *against* prioritizing consumers' economic interests to fight data management regulation. A clearer contextual map of interests could also help judges and regulators in undertaking the law's many formal balancing tests, in areas ranging from consumer protection to antitrust, to determine whether business conduct is appropriate.[304]

Finally, many potential regulatory tools, like data portability, would find support through arguments based in both economics and other norms, such as autonomy.[305] As a result, the expanded mapping of data-related interests may provide the normative force, and a political coalition, necessary to finally bring the kind of omnibus privacy legislation that the field has long proposed.

C. Anti-Pretext Rules

In addition to the more conceptual policy implications outlined so far, privacy pretexts can inform more concrete legal reforms. This section first considers policy responses that would punish or discourage firms from using pretexts. It then moves on to a more promising set of reforms focusing on developing laws that instead target the data management harms that firms advance under the cover of privacy.

1. *Regulating Pretexts*

Should the law police privacy pretexts? Possible paths include new or existing rules related to disclosures, standards of proof, and estoppel. Although offering some promise in theory, each of these approaches has significant practical limits in addressing the big-picture problem.

(1) Disclosures. If companies prominently declare to regulators, businesses, or consumers that they are taking a step to safeguard privacy, they could be required to prominently disclose ulterior data management motives. To illustrate, consider again the email by Bank of America warning its customers of the risks of using third-party services, and encouraging customers to instead use the bank's Security Center.[306] That email only mentioned the benefits to the customer of using the Bank of America portal for all third

---

304 For a discussion of how privacy is typically ignored in the antitrust balancing test, see Douglas, *supra* note 7, at 654.

305 Autonomy is preserved because businesses can still continue to offer the same products and services to the marketplace.

306 *See supra* Part II.

parties.[307] A fuller set of disclosures by Bank of America would acknowledge that using their Security Center would give Bank of America control over whether the third-party app retains access, as well as what information the app can see. The bank could also be required to disclose that it has financial incentives to limit the data available to third-party apps, and that those incentives have the potential to influence the information that Bank of America allows third parties to access. Essentially, the disclosures would give consumers information that would better situate them to decide whether to follow Bank of America's advice to use its Security Center or to instead allow the third-party fintechs direct access to their bank accounts.

Firms could also be required to divulge any acts that are inconsistent with the privacy values they assert. For instance, in announcing new third-party restrictions, Facebook might be required to disclose that it still shares the data with favored third parties. Or a business that is citing privacy to avoid sharing data with a regulator could be forced to divulge that it sells that same requested regulatory data to third parties.

For representations to individuals, existing consumer laws offer a potential response. The prohibition of unfair and deceptive acts is the core of U.S. privacy law and provides a remedy when a business makes deceptive privacy claims.[308] A company telling consumers one thing, as in the Bank of America email, without disclosing as prominently the potential harm, is arguably a deceptive act.[309]

Although disclosures are worth considering, whether they can have much of an impact on this issue is debatable. After all, disclosures have a mixed track record for effectiveness.[310] Moreover, concepts of privacy are excessively complex, causing many scholars exasperation. Consumers will inevitably face difficulty, if not impossibility, in assessing companies' competing privacy claims.[311]

One potential advantageous factor for disclosures in the context of privacy pretexts is that some of the main critiques

---

307 *See id.*

308 *See* Solove & Hartzog, *supra* note 43, at 599.

309 However, the doctrinal path to making that case would likely run into challenges, such as the issue of harm and consumer law's tolerance of omissions rather than misstatements. *Cf.* Citron & Solove, *supra* note 110, at 11 (outlining challenges to establishing the concreteness of many privacy harms).

310 *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 647, 649–51 (2011).

311 *See id.* at 649.

of disclosures are in contexts in which absence of information is the problem.[312] With privacy pretexts, the problem is one-sided information, and it is at least unclear why adding a more balanced communication should overall worsen the informational context for consumers.

(2) Standards of Proof. The law might impose a higher burden of proof on any firm asserting a privacy argument for withholding information from competitors, digital helpers, or regulators. Under a higher standard of proof, the firm might, for instance, be required to establish that the risk of intrusion is substantial and likely. Also, the firm would need to show that the risk cannot be mitigated satisfactorily while handing over the requested information, such as by anonymization.

Inconsistent behavior could also make the privacy claims inherently suspect. Inconsistencies include self-dealing, such as Google citing privacy for not sharing ad click information but then allowing advertisers to purchase that access.[313] Inconsistent privacy conduct would weigh against allowing a privacy defense in court.

(3) Estoppel. Estoppel serves to prevent an entity from taking actions inconsistent with prior behavior. In the context of a firm seeking to withhold information, estoppel might be applied prospectively or retrospectively. Prospectively, the firm might be forbidden from asserting a privacy defense to block information transfer if it has recently taken inconsistent actions, such as sharing the information in question with third parties. Or once a firm has argued privacy as a reason for failing to share information with digital assistants or regulators, it could be prohibited from later sharing that category of information for its own profits. Taken further, this could mean imposing an information fiduciary duty on the firm once it has represented itself as proactively taking steps to protect consumers' privacy from third parties.[314]

Retrospectively, if the firm already shared the requested data with third parties, it would not be allowed to argue in the present instance that it cannot share the information. Inconsistent later sharing of the data might then be subject to disgorgement of profits gained.[315]

---

312 *See id.* at 647, 649–51.

313 *See supra* Part I.

314 On fiduciary duties and duties of loyalty, see Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 966 (2021).

315 Some of these applications may require, or at least benefit from,

Although estoppel would provide a remedy in limited contexts, it is not without drawbacks, such as uncertainty and the potential to discourage privacy innovations within the firm. Another concern is that since firms are often consumers' privacy advocates vis-à-vis the government, the law should be careful not to discourage firms from asserting legitimate privacy interests.

The Limits of Regulating Pretexts. Beyond the localized challenges discussed within the categories above, these legal reforms share more general limits. They would be difficult to enforce, in some cases requiring monitoring or investigations to know when businesses are deploying pretexts. They would add litigation complexity and encourage legal wrangling, which could benefit wealthy firms at the expense of other parties. Also, as illustrated by their application in the context of contracts, disclosure and estoppel are each perhaps too open-ended and dependent on judgment to be administrable, especially at scale.[316] Thus, even with adequate design, it is debatable whether direct regulation of pretexts is worth the resources, especially compared to other approaches discussed below. At best, it would be only a small part of the policy response to privacy pretexts.

2. *Elevating Data Management*

Instead of regulating pretexts, the law could target the heart of the harm by promoting data management. At a minimum, legislatures and regulators would ideally amend existing misappropriated laws to clarify their limits. As one example of reform that is long overdue, the CFAA should be amended to clarify that the statute cannot be used to block the collection of publicly available information, or to prevent consumer-approved access to consumers' own accounts.[317]

More broadly, since the main goal of privacy pretexts is throttling information transfers to undermine data

---

legislation. However, as an equitable remedy, estoppel's reach is potentially broad and well-suited to privacy. *Cf.* Henry E. Smith, *Equity as Meta-Law*, 130 YALE L.J. 1050, 1143–44 (2021) (concluding that equity "solves problems of high complexity and uncertainty that law . . . cannot easily handle" including "polycentricity, conflicting rights, and opportunism.").

316 *See* GRANT GILMORE, THE DEATH OF CONTRACT 61, 72, 88 (Ronald K.L. Collins ed., 1974) (characterizing estoppel as the conclusion that, for reasons the court does not wish to elaborate, judgment must be had for the plaintiff).

317 Orin Kerr has argued against overly broad applications of the CFAA for almost two decades. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1599 (2003).

management, one way to directly address privacy pretexts' harm would be to enact legal rules that explicitly identify allowable information flows, such as originally envisioned through HIPAA. An update to the Administrative Procedure Act and agency-specific information collection statutes could more generally clarify when regulators may collect information despite its link to personal data.[318] Such laws would ideally also emphasize processes for minimizing intrusion risks, such effective anonymization.[319]

An array of other new data management rules could be imagined. The CFPB could write rules promoting open banking, obligating incumbent financial institutions to share customer-requested data with third parties.[320] Stronger interoperability requirements would make it harder for companies to monopolize data or platform access. For example, the bipartisan "Augmenting Compatibility and Competition by Enabling Service Switching Act" would make large platforms allow users to download and transfer their data.[321] A more ambitious move would be to require platforms to allow users to choose the third parties whose algorithms would manage their social media accounts.[322] Related legislation has been proposed that would allow price comparison apps to thrive as well.[323]

Laws promoting data management would, of course, have economic and other justifications beyond solely addressing privacy pretexts.[324] But if information sharing is mandated by law, businesses would have diminished—if not eliminated—

---

318 Any such update should also include a broader set of privacy safeguards. *See* Van Loo, *The Missing Regulatory State*, *supra* note 9, at 1625–27.

319 Anonymization has limits, but those limits have been exaggerated because of some anecdotal early failed efforts that had employed flawed designs. *See, e.g.*, Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 708–09 (2016) (outlining the importance of anonymization).

320 *See* Van Loo, *Making Innovation More Competitive*, *supra* note 7, at 267 (critiquing the CFPB for not writing open banking rules and pointing out that such rules are necessary for competition). For a more comprehensive proposal for open banking, see Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 328, 383 (2021).

321 Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, S. 2658, 116th Cong. §§ 2(7)(b), 3(a).

322 The Act has elements of this, but this concept is more fully reflected in a recent scholarly proposal. *See* Fracassi & Magnuson, *supra* note 320 (providing a mechanism for users to enlist third-party data custodians that could manage access to multiple social networks); FUKUYAMA ET AL., *supra* note 166, at 32 (proposing "middleware" algorithms to allow users greater control over their data and access to online information).

323 S. 2658, 116th Cong. § 5 (2019).

324 *See supra* Part I & subpart III.B.

motives for crafting privacy pretexts because doing so would not insulate them from allied access.

D. Policy Making with Privacy Pretexts in Mind

Policy makers should consider privacy pretexts when enforcing or creating legal rules. That means clearly thinking through potential rhetorical guises and delineating acceptable uses of the legal rules. Minding privacy pretexts is important because each new enforcement action or written rule increases the risks of extending more pretext-driven control to companies over contextual information norms. For instance, the most prominent and far-reaching U.S. privacy enforcement action, the FTC's Cambridge Analytica settlement order with Facebook, required the social network to monitor third parties' privacy compliance.[325] That requirement gave the social network an authoritative source—a binding court order—that the company later used to justify blocking academic researchers while gathering more data from competitors that use its platform.[326] The FTC order was focused on anti-intrusion and demonstrated limited awareness of data management.[327]

Data management considerations are especially important to keep in mind in any anti-intrusion legislation or rulemaking. Historically, as discussed above, the opposite occurred—addressing anti-intrusion when legislating data management.[328] When data management concerns motivated legislation, as with HIPAA, lawmakers felt compelled to add on anti-intrusion rules. However, when the main impulse was anti-intrusion, as with the CFAA, lawmakers were more likely to ignore data management.[329] Greater attention symmetry to these two sides of information flow is warranted.

As part of this balance, a privacy law regime must have a sense of market failures. Taken too far, privacy policies emphasizing non-economic rights and control risk providing a

---

325 *See* Consent Order §§ 2–3, *In re* Google Inc., File No. 102-3136 (F.T.C. Mar. 30, 2011).

326 *See* Horwitz, *supra* note 206.

327 In terms of third-party access, the settlement relied on Facebook hiring a third-party auditor. That meant the auditor would be friendly to Facebook, who was then a client to the auditor. And the auditor did not even have access, as it instead relied on representations by Facebook to ensure compliance. *See* Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders* 4, 6 (Apr. 2018) (unpublished manuscript), https://ssrn.com/abstract=3165143 [https://perma.cc/QNX4-CXDR].

328 *See supra* Part I.

329 *See id.*

pyrrhic victory. Consumer advocates would feel like they have won because of data security standards and strict prohibitions against unauthorized sharing of data with third parties. Dominant businesses could also feel like they have won. They need to invest in data security anyway, so that is not necessarily a concession.[330] And incumbent businesses would have gained a powerful anti-intrusion norm for cementing their market positions. Thus, any comprehensive privacy legislation should also target any potential accompanying market failures. Doing so could forestall privacy pretexts resulting from the new rules.

Another way of viewing this state of affairs is that the absence of comprehensive privacy legislation facilitates privacy pretexts. The more contexts that are clearly covered by strong data management and anti-intrusion rules, the less leeway companies have to misdirect the normative conversations.[331] Such comprehensive legislation also can limit industry capture of the regulatory process, albeit imperfectly.[332] If laws state clearly that regulators can collect certain categories of information, for instance, the captured regulator has less of an opening to use privacy as a pretext for not collecting that information.

Again, greater attention to data management does not mean weak anti-intrusion rules. Viewed through an extreme anti-intrusion lens, these two faces of privacy are incompatible. For instance, a universal anti-intrusion regime would prohibit all allied access. However, that extreme does not reflect the field of privacy. Striking the balance between these two sets of data interests will no doubt at times require difficult tradeoffs.[333] The involvement of an appropriately resourced and authorized regulator would help in managing these points of tension. That regulator could help adjust the laws as businesses inevitably attempt to strategically maneuver around them.

On the matter of tensions between data management and anti-intrusion, it helps to consider the policy baseline. The

---

330 Security is important for customer relations, and it is difficult to regulate the level of security taken. Thus, investing in security is not a huge concession.

331 Indeed, the same can be said for vague anti-intrusion statutes, which businesses have used to undermine anti-intrusion protections. *See* Waldman, *supra* note 5, at 797–98.

332 For a helpful background review of the relevant literature, see Wiener & Richman, *supra* note 44.

333 Indeed, at least some of the criticism about the GDPR reflects the tension between its data management and anti-intrusion sides.

U.S. privacy framework is overall quite limited. As a practical matter, a comprehensive mapping of privacy interests could provide a blueprint for legislation with significantly stronger anti-intrusion and data management laws, as other countries have adopted.[334] At a minimum, reflecting on how businesses might seek to block beneficial information flows would lessen the chances that the privacy movement's success causes unintended harms.

So far, this discussion has focused on making privacy law. But there is a broader context that helps to underscore why privacy pretexts merit attention in policy making. Over the past several centuries, private sector mobilization of the law has repeatedly facilitated large-scale economic transitions. Property laws played a key role in allowing the enclosure of the British commons.[335] Labor laws paved the path for the Second Industrial Revolution.[336]

Scholars have shown how firms have more recently used legal entrepreneurship to set the stage for the rise of the information economy. Intellectual property laws allowed a kind of "second enclosure" of the intellectual commons.[337] And platforms like Uber have exploited loopholes in the law and then mobilized their constituents to lobby for favorable legal changes.[338]

Privacy pretexts provide another example of such legal mobilization, whether as part of that second enclosure, or as a new third enclosure movement.[339] They allow firms to

---

334 Statutes are possible that have strong rules guarding both sets of interests, as demonstrated by the GDPR. The GDPR limits what businesses can do with data, especially without being candid, but still gives consumers strong portability and access. *See* GDPR, art. 15, 20, 2016 O.J. (L 119) 38 (EU).

335 *See* Dan Bogart & Gary Richardson, *Property Rights and Parliament in Industrializing Britain*, 54 J.L. & ECON. 241, 247–48 (2011).

336 As did the capital formation framework. *See* HARRY BRAVERMAN, LABOR AND MONOPOLY CAPITAL: THE DEGRADATION OF WORK IN THE TWENTIETH CENTURY 125, 251–69 (1974).

337 *See* James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 L. & CONTEMP. PROBS. 33, 37 (2003).

338 *See* Pollman & Barry, *supra* note 44, at 446.

339 On the one hand, whereas the second enclosure was more content-focused, the third enclosure may be more data-focused, as several recent scholarly observations can be classified. *See* COHEN, *supra* note 5, at 68–79 (showing how platforms have repurposed laws to control data); *cf.* Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1397, 1399 (2021) (observing a broader return to walled gardens, due largely to nations erecting barriers). On the other hand, James Boyle foreshadowed many of these tools of information exclusion in observing the second enclosure movement in the 1990s and 2000s. *See* BOYLE, *supra* note 44, at 182 (observing that "the idea that personhood entails control over information . . . might seem" to pose "a challenge to the distribution of power

entrench their market positions by enclosing their data from third parties. The ability to block disruptive apps like Power Ventures, the social media tool, enabled stronger walls around incumbents like Facebook.[340]

Privacy pretexts also fit into the second act of each of these economic revolutions—the legal countermovement. The enclosure of the commons and the industrial revolution caused such significant upheaval that diverse actors responded with protective measures. Muckraking journalists exposed slaughterhouse filth and anticompetitive monopolies.[341] Grassroots organizations launched educational campaigns about toxic waste dumps.[342] And Congress massively expanded legal protections.[343] The beginnings of related responses to information economy discontents can now be seen.

In that historical context, privacy pretexts can be viewed as an overlooked tool for mobilizing norms to undermine the accountability countermovement. Allied access is key to accountability, particularly regulators and digital tools. Furthermore, to have enough incentive to mobilize politically, harmed individuals must have some way of knowing they are being harmed. Yet businesses have also used privacy pretexts to block journalists, academics, and nonprofits seeking access for the purpose of assessing what businesses are doing with information.[344] Information accountability must be dispersed and polycentric, but privacy pretexts undermine the accountability of diverse actors.[345]

These specific tactics are important, but they are only the most visible part of how privacy pretexts ward off a countermovement. Privacy pretexts are concerning not only

---

in society").

340 *See supra* subpart II.A.

341 *See generally* IDA M. TARBELL, 2 THE HISTORY OF THE STANDARD OIL COMPANY 85 (1904); UPTON SINCLAIR, THE JUNGLE 109–17 (1906). On countermovements more broadly, see, for example, COHEN, *supra* note 5, at 5–8.

342 Sheila Foster, *Justice from the Ground Up: Distributive Inequities, Grassroots Resistance, and the Transformative Politics of the Environmental Justice Movement*, 86 CALIF. L. REV. 775, 813 (1998).

343 *See, e.g.*, *Hearings Before the H. Comm. on Agric. on the So-called "Beveridge Amendment" to the Agricultural Appropriation Bill*, 59th Cong. 94, 102 (1906) (statement of Charles P. Neill).

344 *See supra* section II.A.2.

345 On the importance of pluralistic accountability, see, for example, Carla L. Reyes & Jeff Ward, *Digging into Algorithms: Legal Ethics and Legal Access*, 21 NEV. L.J. 325, 325 (2020) (arguing that lawyers and non-technologists alike must collectively "focus on understanding algorithmic systems as technology created, manipulated, and used in a particular context").

for what conduct they may allow now or in the future. They are also noteworthy because they are laying linguistic and normative foundations before any real legal countermovement has formed. Anti-intrusion and data management will lie at the core of any substantial renovations to the legal architecture. Privacy ploys may thus shape the coming construction of a legal framework for responding to data economy discontents.

It is also worth noting that one feature separates privacy pretexts from some of the other instances of businesses mobilizing laws in societally harmful ways. In the case of free speech, intellectual property, and transparency laws, the main move is for businesses to assert their own entitlements under those laws.[346] With privacy pretexts, businesses are instead asserting themselves as protectors of individuals' privacy. In other words, whereas transparency and speech assert the legal rights of a small number of business owners, privacy pretexts are more dangerously cloaked as advancing the rights of the masses. That difference gives privacy pretexts the potential to have greater normative reach and staying power.

For these reasons, the project of elevating privacy pretexts in the minds of lawmakers, judges, and regulators has a potentially important legal role to play. Although they are presumably uncoordinated instances of actors aggressively pursuing their self-interests, privacy pretexts nonetheless may exert a powerful collective influence. Seemingly subtle decisions about whether to embrace economic rationales and whether to emphasize allied access can rearrange policy makers' design decisions. Exposing the systemic anti-intrusion opportunism lessens the chance that businesses reorient privacy in opposition to data optimality.

CONCLUSION

This Article has shown how businesses repurpose privacy to shape the contextual norms that govern information flows. They use that control to erect walls around their data, thereby excluding key actors, such as competitors, digital helpers, researchers, and regulators. Understanding the architecture of those digital fortresses reveals deeper challenges to the information society.

---

346 *See* BOYLE, *supra* note 44, at 13; Boyle, *supra* note 337, at 33; COHEN, *supra* note 5, at 5–8, 257. On how businesses have become the primary beneficiaries of FOIA, see Margaret B. Kwoka, *Inside FOIA, Inc.*, 126 YALE L.J. F. 265, 266 (2016).

Privacy pretexts operate by reframing societally beneficial data sharing as an intrusion on the individual. The privacy framework's skepticism of third-party access facilitates that equivocation. So does the lack of attention to economic arguments. Those two factors, along with the field's expansive definition, have left the norms for data management less developed, and thus more vulnerable to obfuscation. The enormous task of designing data regulation would be challenging enough with linguistic and conceptual clarity. Businesses' rhetorical distortions warp the normative and legal framework upon which reforms will build.

Data management principles are too societally important to be systematically sidelined by privacy's pathologies. Fortunately, these two faces of data interests need not persist in an irreconcilable state of tension. No universal principle requires the law to allow incumbent businesses to strategically choose between the free flow of information and enclosure.

Attentiveness to privacy pretexts in rhetoric, rulemaking, and enforcement is the first step. Caution about pretexts need not halt privacy's progress, but should instead inform its shape. A greater emphasis on the economic arguments in favor of data management's collective goals would offer a more promising path forward for governing data in the twenty-first century. Whatever the normative foundation, network technologies' core societal contribution is to bring people together. A strong principle of allied access would make it harder for these technologies to be used as tools of isolation.