PRIVATE RIGHTS OF ACTION IN PRIVACY LAW

LAUREN HENRY SCHOLZ*

ABSTRACT

Many privacy advocates assume that the key to providing individuals with more privacy protection is strengthening the government's power to directly sanction actors that hurt the privacy interests of citizens. This Article contests the conventional wisdom, arguing that private rights of action are essential for privacy regulation. First, I show how private rights of action make privacy law regimes more effective in general. Private rights of action are the most direct regulatory access point to the private sphere. They leverage private expertise and knowledge, create accountability through discovery, and have expressive value in creating privacy-protective norms. Then to illustrate the general principle, I provide examples of how private rights of action can improve privacy regulation in a suite of key modern privacy problems. We cannot afford to leave private rights of action out of privacy reform.

* McConnaughhay and Rissman Professor, Florida State University College of Law. Many thanks to the following for their comments and conversations: Aditi Bagchi, Daniel Solove, Lisa Austin, Julie Cohen, Ryan Calo, Mark Bauer, Pamela Bookman, Thomas Lee, Ronald Mann, Gus Hurwitz, David Thaw, Thomas Kadri, Sabine Tsuruda, Hannah Bloch-Webha, Andrew Selbst, Xiyin Tang, and participants in workshops hosted by USC Gould School of Law, Fordham Law School, Nebraska College of Law, and the AALS Sections on Commercial and Consumer Law.

TABLE OF CONTENTS

INTRODUCTION

Federal privacy legislation in the United States is coming.[1] This will place the United States in step with the global zeitgeist. In the past few years, many jurisdictions, including the European Union, Brazil, China, Canada, and Australia, have passed comprehensive privacy legislation.[2] In 2018, California passed comprehensive privacy legislation—which has been influential beyond the state's borders[3]—and ten more states are on track to pass privacy legislation this year.[4] Increased enforcement of consumer privacy rights in these jurisdictions has led industry to actively lobby Congress for federal legislation on privacy, seeking simplification of the patchwork of laws with which potentially regulated companies must comply.[5] Industry is now on the same page as American consumer advocates who have long advocated for a federal privacy law.[6] There is bipartisan political consensus around the need for federal privacy

1. Karen Schuler, *Federal Data Privacy Regulation Is on the Way—That's a Good Thing*, IAPP (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/ [https://perma.cc/GJV9-M5XT].

2. *See Global Comprehensive Privacy Law Mapping Chart*, IAPP, https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf [https://perma.cc/5C9S-CBCL].

3. Brandon P. Reilly & Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020), https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed [https://perma.cc/C6X2-P2FG].

4. Ruth Reader, *These States Are on Track to Pass Data Privacy Laws this Year*, FAST CO. (Feb. 24, 2021), https://www.fastcompany.com/90606571/state-data-privacy-laws-2021 [https://perma.cc/TYF9-MRBU] (describing content and status of legislation recently passed or set to pass in Nevada, Vermont, Maine, Virginia, New York, Washington, Utah, and Oklahoma, and noting that Alabama, Arizona, Florida, Connecticut, and Kentucky all have bills on the docket that follow a similar format to California's California Consumer Privacy Act).

5. *Business Roundtable CEOs Call on Congress to Pass Comprehensive, Nationwide Consumer Data Privacy Law*, BUS. ROUNDTABLE (Sept. 10, 2019), https://www.businessroundtable.org/business-roundtable-ceos-call-on-congress-to-pass-comprehensive-nationwide-consumer-data-privacy-law [https://perma.cc/8PT3-TZBY]; David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018, 6:30 AM), https://fortune.com/2018/11/29/federal-data-privacy-law/ [https://perma.cc/6AA6-K5SW].

6. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 15-19 (2019) (interviewing many privacy experts who advocate for the need for federal legislation on privacy); *see also* Alexandria J. Saquella, Comment, *Personal Data Vulnerability: Constitutional Issues with the California Consumer Privacy Act*, 60 JURIMETRICS 215, 231-32 (2020).

legislation, with politicians of both parties concerned about abuse of power by Big Tech.[7]

There is a great deal of consensus around the ground a federal privacy law should cover.[8] Companies are amenable to an understanding that notice and choice are insufficient to delineate privacy rights in an interconnected world and even that fiduciary duties may exist between firms and consumers with respect to personal information.[9] But two principal fault lines are holding up legislative action: preemption and private right of action.[10] In privacy law, there is extensive scholarly debate on the question of preemption.[11] By contrast, there is scant discussion of the need for expanding the ability of private actors to enforce privacy protections.[12]

---

7. Schuler, *supra* note 1.

8. Elizabeth R. Pike, *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, 69 EMORY L.J. 687, 720 (2020).

9. *See generally* Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19 (2021) (describing the evolution in corporate rhetoric about their privacy obligations from lassiez-faire ideology, which saw a need for only minimal notice and choice obligation at most, to today's neoliberal rhetoric, which contends internal corporate compliance structures can protect privacy).

10. *See* Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 547-48 (2020); Peter Swire, *US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws*, IAPP (Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/ [https://perma.cc/9QJE-AEP9].

11. Swire, *supra* note 10; Peter Swire, *US Federal Privacy Preemption Part 2: Examining Preemption Proposals*, IAPP (Jan. 10, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals/ [https://perma.cc/9BWE-B8FC] (outlining the basic terms of the preemption debate and evaluating legislative proposals). The conversation about the trade-off between allowing legislative innovation to proceed in the states and providing certainty to industry predates the current moment. *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904-06 (2009).

12. *See* Soubouti, *supra* note 10, at 547 ("While some states provide consumers with a private right of action, most notably the [California Consumer Privacy Act of 2018], none of the current federal legislative proposals offer this source of accountability to allow consumers to take companies to court for federal privacy law violations." (footnote omitted)). A handful of scholars have highlighted the role of private rights of action, and they also often note the dearth of scholarship on the topic. *See, e.g.*, Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1929-32 (2019); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614, 619-22 (2018); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1850-52 (2010); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 283, 292-93 (2007) [hereinafter Citron, *Reservoirs of Danger*]; Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 144-46 (2006).

For example, Florida appeared to be on the verge of passing an ambitious and effective state privacy law, but disagreement over a private right of action stymied the bill. The Florida House passed a privacy bill that would have provided citizens with a set of substantive privacy rights, authorized the attorney general to police violations, and granted Florida citizens a private right of action.[13] With the support of Governor Ron DeSantis, the bill passed the Florida House almost unanimously, 118-1.[14] Many House members were eager to provide Floridians with protections against a technology sector they saw as exploitative and overreaching.[15] Due to industry pressure, the House privacy bill died in the Senate. Instead, the Florida Senate passed a similar privacy bill sans private right of action.[16] The House refused to pass the Senate version of the bill, and the legislation died.[17] As one industry commentator observed: "the Florida bill died because the House and Senate could not align on a private right of action—in other words, an individual's ability to sue a company for privacy damages. The Senate's version of the

---

Even when private law approaches come up, they are usually as an afterthought. *See, e.g.*, Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 669-70 (2019) ("To be clear, this Article primarily addresses the companies' relationships to governments. It does *not* focus on the many significant issues surrounding technology companies' relationships with their users in general, though as the Conclusion highlights, the rise of Digital Switzerlands may have implications for company-user dynamics as well." (footnote omitted)). This mentality is far from unique to privacy scholarship. As Hanoch Dagan and Avihay Dorfman observed, "[a] well-ingrained notion in liberal-egalitarian thought is that the state's responsibility to ensure fair equality of opportunity is sufficient for realizing substantive equality and freedom." Hanoch Dagan & Avihay Dorfman, *Just Relationships*, 116 COLUM. L. REV. 1395, 1402 (2016).

13. Susan Grant & Caitriona Fitzgerald, *Florida's Privacy Bill Needs Teeth Back or It's 'Protections' Are Meaningless*, TALLAHASSEE DEMOCRAT (Apr. 23, 2021, 6:30 AM), https://www.tallahassee.com/story/opinion/2021/04/23/florida-senate-must-put-private-right-action-back-privacy-bill/7323010002/ [https://perma.cc/L3CE-V3JR]; News Service of Florida, *Florida Gov. DeSantis Continues Targeting Big Tech, Pushes Data Privacy Legislation*, TALLAHASSEE DEMOCRAT (Feb. 16, 2021, 6:01 AM), https://www.tallahassee.com/story/news/2021/02/16/florida-gov-desantis-continues-targeting-big-tech-data-privacy-legislation-fiona-mcfarland-sprowls/6758908002/ [https://perma.cc/5RGH-4K4R].

14. Grant & Fitzgerald, *supra* note 13; News Service of Florida, *supra* note 13.

15. News Service of Florida, *supra* note 13; Benjamin Freed, *Florida Privacy Bill Tanks over Individuals' Right to Sue*, STATESCOOP (May 6, 2021), https://statescoop.com/florida-privacy-bill-tanks-private-right-action/ [https://perma.cc/BW77-5MTY].

16. Grant & Fitzgerald, *supra* note 13.

17. Kendra Clark, *Florida State Privacy Bill Squashed After Backlash from Local Businesses*, THE DRUM (May 4, 2021), https://www.thedrum.com/news/2021/05/04/florida-state-privacy-bill-squashed-after-backlash-local-businesses [https://perma.cc/77DK-FNNZ].

bill removed the private right of action, and House members clearly felt this left the law toothless."[18] At the time of this writing, the debate is still ongoing.[19] Debates like the one in Florida are happening throughout the country,[20] so it is critical to understand what is at stake when privacy legislation includes—or omits—a private right of action.

In providing a framework for understanding the role of private enforcement in privacy regulation, this Article both fills an important gap in the legal literature and addresses a contemporary policy question.[21] Private rights of action have two important benefits for privacy regulation.

First, private enforcement marshals the resources of the private sector to fund and provide information in dealing with this ubiquitous issue. Private enforcement and public enforcement are complements not substitutes. Addressing modern privacy problems requires productive redundancy—that is, providing legal avenues for both government and private parties to observe and challenge privacy-invasive practices.[22] The hybrid approach has precedent in regulatory areas such as employment, civil rights, and consumer protection. The two avenues of enforcement reinforce each other.

---

18. *Id.*

19. Joseph Duball, *Florida Privacy Bill Maintains PRA Ahead of House Floor Vote*, IAPP (Feb. 24, 2022), https://iapp.org/news/a/florida-privacy-bill-maintains-pra-ahead-of-house-floor-vote/ [https://perma.cc/29UX-P3GK].

20. Freed, *supra* note 15.

21. I follow other commentators in characterizing the system of rules for use of a statutorily created private right of action as a "private enforcement regime." *E.g.*, Stephen B. Burbank, Sean Farhang & Herbert M. Kritzer, *Private Enforcement*, 17 LEWIS & CLARK L. REV. 637, 639 n.2 (2013) ("We use the phrase 'private enforcement' for both enforcement initiated by private parties but taken over by public officials as well as enforcement initiated and prosecuted by private parties. We use the phrase 'private enforcement regime' to refer to the system of rules that a legislature includes in its statutory design after deciding to include a private right of action.").

22. *See* Zachary D. Clopton, *Redundant Public-Private Enforcement*, 69 VAND. L. REV. 285, 318-20 (2016) (establishing redundant public-private enforcement as common in the regulatory status quo and suggesting it as a proper strategy for regulating important interests); *see also* Elysa M. Dishman, *Enforcement Piggybacking and Multistate Actions*, 2019 BYU L. REV. 421, 424, 430 ("The multienforcer system provides accountability by allowing other enforcers to step in to remedy lackluster enforcement resulting from problems of agency capture, resource constraints, informational disadvantages, and political impediments.... When all enforcers focus their resources and efforts on large corporate targets, it deprives enforcement resources from other targets that may cause more localized harm but lack the deep-pockets to pay large fines or create splashy headlines.").

The modern American administrative state is not capable of addressing an issue of information privacy's magnitude without support from private enforcement.

Second, private rights of action have expressive value that cannot be achieved through public regulation in the area of privacy.[23] The nature of the right implies that an individual opportunity to be heard should be available. Privacy is a personal, dignitary right, so there should be some avenue for an individual to personally contest privacy violations. The ability to bring a claim is itself a recognition of the dignity of the plaintiff.

Understanding the key contributions of private enforcement to privacy regulation leads to several implications. First, because the success of a private enforcement regime is based on its actual availability, neither enforcement support nor dignitary concerns will be served by private rights of action that are in practice unavailable. Any private enforcement avenue should address access to justice concerns. Examples of provisions that increase the accessibility of litigation include fee-shifting arrangements and elevated remedies. Second, understanding what private enforcement contributes to privacy regulation allows stakeholders to understand what limits on private enforcement are possible without undermining the goals of a private right of action. Limited private rights of action, such as a right to explanation or a right to deletion, can relieve administrative agencies of the burdens of addressing smaller matters and affirm individual dignity. Several statutes have limited their application to larger companies, making sure the burden of enforcement falls on the companies most able to fund the public good of litigation on the topic. This is compatible with the aim of having a resilient private partner for public regulators in enforcement. But it does run afoul of the second function of private enforcement, which is to affirm the dignity of citizens by allowing them access to civil recourse when it comes to their personal right of privacy.

This last point reveals that the twin purposes of private enforcement that this Article has identified can be in tension. An individual plaintiff vindicating her own rights may not always have the public

23. *Cf.* J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137, 1153-60 (2012) (showing the essential role of private enforcement through litigation in the functioning of the modern administrative state).

interest in mind in how she chooses to resolve them. Private enforcement regimes tailored to provide support to public enforcement of matters of public concern may not always provide direct claims for relief for wronged citizens due to countervailing considerations. Lawmakers must consider both purposes of private enforcement in privacy regulation and balance accordingly between the two when considering the scope of private rights of action. For example, the dignitary interest may be more dominant for framing private enforcement of sexual privacy intrusions, whereas providing regulatory resilience may be more significant for private enforcement of anticompetitive data power claims.

The Article proceeds as follows. Part I shows that a hybrid enforcement regime—a regulatory regime that has both private and public enforcement avenues—is a more effective regime for privacy enforcement than purely public enforcement. Part II argues that the dignitary concerns implicated by privacy invasions independently counsel for the availability of civil recourse via private enforcement. Part III illustrates the critical role private rights of action can play in five important privacy problems of the day.

I. COMPARING PRIVATE, PUBLIC, AND HYBRID ENFORCEMENT OF PRIVACY LAW

Hybrid enforcement is needed for privacy regulation in the United States. The Federal Trade Commission (FTC) is "the largest and arguably the most important component of the U.S. privacy regulatory system."[24] Furthermore, Danielle Citron's work shows that state attorneys general also play a key role in enforcing privacy law.[25]

These public enforcers play a critical role in privacy regulation and should continue to do so. Yet private enforcement is necessary to support public enforcement. Private enforcement deters potential wrongdoers by allowing for a resilient avenue of enforcement, available even when agency funding or political will is lacking. It

24. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

25. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748-51, 755-57 (2016).

also broadens and democratizes the public forum for sharing and analyzing disputes in the information economy beyond the limits of administrative agencies. Matters brought to light by private enforcers, even if they are unsuccessful in their efforts, can aid public enforcers in their regulatory choices.

Private rights of action have long been a prominent tool in American regulation.[26] Since the mid-twentieth century, there has been increasing reliance on private rights of action to achieve regulatory goals.[27] As Sean Farhang put it, in lieu of a European-style regulatory state, the American system has a litigation state.[28] Enthusiasm for private rights of action crosses ideological lines, with conservatives and liberals alike seeking to use private enforcement to shore up important rights.[29] Regulation in substantive areas that include both private rights of action and public enforcement have been dubbed "hybrid [enforcement] regimes."[30] These hybrid enforcement regimes exist in antitrust, securities, civil rights, employment, and consumer protection, among others.[31] There is expressive value to giving individuals the right to seek relief from those that have wronged them that is not replicated in public enforcement.[32] Yet, even if one doubts that private enforcement offers unique benefits, it is apparent that the public enforcement system in the United States is reliant for its effectiveness upon private enforcement systems in many areas of complex regulation.[33] Absent a rehaul of our public administrative systems,

---

26. *See, e.g.*, Aditi Bagchi, *Distributive Injustice and Private Law*, 60 HASTINGS L.J. 105, 111 (2008).

27. *See* Kit Barker, *Private Law: Key Encounters with Public Law*, *in* PRIVATE LAW: KEY ENCOUNTERS WITH PUBLIC LAW 3, 5-12 (Kit Barker & Darryn Jensen eds., 2013). Scholars have posited several reasons behind this shift. Glover, *supra* note 23, at 1151-52 (describing several possible explanations, including lack of public capacity, legislative desire to avoid administrative burdens, and legislative desire to avoid blame for unpopular administrative moves).

28. SEAN FARHANG, THE LITIGATION STATE: PUBLIC REGULATION AND PRIVATE LAWSUITS IN THE U.S. 214 (2010).

29. Stephen B. Burbank & Sean Farhang, *A New (Republican) Litigation State?*, 11 U.C. IRVINE L. REV. 657, 684, 686 (2021).

30. Clopton, *supra* note 22, at 292.

31. *Id.* at 295-98.

32. *See* discussion *infra* Part II.

33. *See* FARHANG, *supra* note 28, at 214-16.

relying on public enforcement alone is unlikely to be as effective as a hybrid regime.[34]

This Part will describe examples of public enforcement regimes in privacy law, then private enforcement regimes, pointing out the limitations of each. I will then show that the existing hybrid enforcement regimes in privacy regulation have proven more successful than regimes that choose just one avenue of enforcement, and suggest that the benefits of hybrid regulation provide an explanation for their greater success.

A. Public Enforcement Regimes

Three examples of privacy regulations that are publicly enforced are: the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the FTC's authority to regulate "unfair and deceptive" business practices.[35]

HIPAA provides rules and regulations governing how medical providers handle and process personal health information.[36] It creates civil and criminal penalties for wrongfully disclosing personal health information and authorizes the Department of Health and Human Services (HHS) to promulgate regulations to protect health privacy.[37] HHS and state attorneys general enforce the statute and corresponding regulations.[38] A recent empirical study of HIPAA enforcement actions showed that "HHS and state attorneys general focus their settlement and penalty efforts on cases involving groups ... of patients and insureds," and usually do not take action on behalf of "individuals whose privacy and security rights have

---

34. *See id.* (crediting the success of Title VII to implementation through a private/public law regime).

35. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/XFT8-75VZ].

36. Beverly Cohen, *Reconciling the HIPAA Privacy Rule with State Laws Regulating Ex Parte Interviews of Plaintiffs' Treating Physicians: A Guide to Performing HIPAA Preemption Analysis*, 43 HOUS. L. REV. 1091, 1095-1105 (2006) (describing the HIPAA privacy rule).

37. 42 U.S.C. § 1320d-5 ("General penalty for failure to comply with requirements and standards"); *id.* § 1320d-6 ("Wrongful disclosure of individually identifiable health information").

38. *Id.* § 1320d-6; Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010).

been violated."[39] There is no private right of action under HIPAA's privacy rule for individuals whose health information is compromised.[40]

COPPA limits personal information gathering from children under the age of thirteen on the internet.[41] The statute directs the FTC to issue and enforce regulations against noncomplying companies.[42] The FTC provides guidance on protecting children's privacy.[43] Only the FTC and state attorneys general may bring enforcement actions against firms for COPPA violations.[44] There is no private right of action for children whose personal information is compromised under COPPA regulations.[45]

The Federal Trade Commission Act authorizes the FTC to regulate "unfair and deceptive acts or practices."[46] Unlike HIPAA and COPPA, the FTC's authority to regulate these business practices is general, not limited to a particular sector or class of beneficiaries.[47] A broad body of law has cropped up. However, because Congress granted this authority to the FTC, there is no private right for individuals to sue for unfair and deceptive practices under FTC guidance, precedent, and regulations.[48]

---

39. Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. 1361, 1374-90 (2019).

40. Acara v. Banks, 470 F.3d 569, 571-72 (5th Cir. 2006) ("Every district court that has considered this issue is in agreement that the statute does not support a private right of action.").

41. 15 U.S.C. § 6501(1) (defining the term "child" to mean "an individual under the age of 13"); *id.* § 6501(10)(A) (stating that a "website ... directed to children" is "a commercial website or online service that is targeted to children ... or ... [a] portion of a commercial website or online service that is targeted to children").

42. *Id.* § 6502(b)(1).

43. *E.g.*, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/AP3D-7JW2] [hereinafter FTC COPPA Compliance Plan].

44. *See, e.g.*, Jesse M. Brody, *Parents Sue TikTok for COPPA Violations, Settle for $1.1M*, MANATT (Dec. 17, 2019), https://www.manatt.com/insights/newsletters/advertising-law/parents-sue-tiktok-for-coppa-violations-settle [https://perma.cc/X4EA-VWWG].

45. *See id.* (explaining how, although there is no private right of action under COPPA, plaintiffs have leveraged the FTC's COPPA actions to gain settlements under common law privacy tort theories).

46. Federal Trade Commission Act, 15 U.S.C. §§ 41-58.

47. *Compare id.* § 45, *with* 42 U.S.C. § 1320d-6, *and* FTC COPPA Compliance Plan, *supra* note 43.

48. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N app. B (May 2021), https://www.ftc.gov/

Under these three public privacy laws, a government actor discovers and takes action against private actors that violate statutory or regulatory privacy rules.[49] The FTC has been the primary source of privacy regulation in the United States to date,[50] with state attorneys general playing a significant supporting role.[51] However, it also has significant limits. The FTC is a "norm entrepreneur," not police; its goal is not to take action against every violator of the rules, but to encourage every actor to improve their practices in reference to a relatively small number of actions.[52] Some commentators argue that this system, without modifications, encourages capture and laxity.[53] Others suggest the penalties carried by enforcement are simply too small.[54] The FTC itself admits that it needs more resources to adequately regulate privacy.[55] HIPAA and COPPA have had substantial problems adequately protecting health and children's privacy, respectively, and have been subject to extensive critiques on their basic effectiveness.[56] Both programs

about-ftc/what-we-do/enforcement-authority [https://perma.cc/YN9A-VGW2]. Individual states have common law actions against fraud and consumer protection statutes barring wrongful behavior; individual plaintiffs may rely on FTC precedent as persuasive authority in such actions but their claim does not have its source in the FTCA. *See, e.g.*, VA. CODE ANN. § 59.1-204 (2021); Mason v. Mortgage Am., Inc., 792 P.2d 142, 149 (Wash. 1990) (en banc).

49. *See supra* notes 35-48 and accompanying text.

50. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2045-46 (2000).

51. Citron, *supra* note 25, at 748, 750, 811 (empirical study describing the role state attorneys general play in privacy regulation).

52. *See* Hetcher, *supra* note 50, at 2045-46.

53. *See, e.g.*, William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 964 (2016) (addressing skeptics of the American model of regulation and encouraging responsive regulation as a way to improve it).

54. *See, e.g.*, Solove & Hartzog, *supra* note 24, at 605-06.

55. Aaron Nicodemus, *FTC Stumps for Additional Resources to Police Privacy*, COMPLIANCE WK. (June 23, 2020, 2:41 PM), https://www.complianceweek.com/data-privacy/ftc-stumps-for-additional-resources-to-police-privacy/29108.article [https://perma.cc/U88G-CGZ2].

56. *E.g.*, Morgan Leigh Tendam, Note, *The HIPAA-Pota-Mess: How HIPAA's Weak Enforcement Standards Have Led States to Create Confusing Medical Privacy Remedies*, 79 OHIO ST. L.J. 411, 419-22 (2018) (arguing that HIPAA's current enforcement scheme does not go far enough to protect medical privacy or provide adequate remedies to victims of HIPAA violations); Shannon H. Houser, Howard W. Houser & Richard M. Shewchuk, *Assessing the Effects of the HIPAA Privacy Rule on Release of Patient Information by Healthcare Facilities*, 4 PERSPS. HEALTH INFO. MGMT. 1, 1-5 (2007); Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 541-48 (2007) (critiquing COPPA as limited by "linear assumptions about development"); Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 775 (2001) ("Privacy advocates are

suffer from being limited in scope due to sector and age limitations, and contain loopholes that enable actors in the industry to strategically evade coverage.[57] For example, websites have been able to avoid the COPPA privacy regulations by simply requiring each user to claim they are over thirteen, without confirming the validity of the user's purported age.[58]

Public enforcement of privacy law simply has not proven expansive or resilient enough to create accountability and deter wrongful practices.

B. Private Enforcement Regimes

Three examples of private enforcement regimes in privacy law include the Video Privacy Protection Act of 1988 (VPPA),[59] state common law privacy torts,[60] and trade secret law.[61]

VPPA bars "video tape service provider[s] ... [from] knowingly disclos[ing] ... personally identifiable information concerning any consumer" to a third party.[62] VPPA authorizes consumers to sue when a video tape service provider discloses personal information.[63] Despite the statute's reference to video tapes, it can and has been used by consumers to protect their privacy interest in protecting

---

not so sure about COPPA, despite the characterization of its passage as a consumer privacy victory."). *But see* Mark A. Rothstein, *The End of the HIPAA Privacy Rule?*, 44 J.L. MED. & ETHICS 352, 352 (2016) ("Ever since the ... [HIPAA] Privacy Rule took effect in 2003, it has been one of the most misunderstood and disrespected of federal regulations." (footnotes omitted)).

57. Rothstein, *supra* note 56, at 352-53, 357.

58. Shannon Finnegan, Comment, *How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future*, 50 SETON HALL L. REV. 827, 828 (2020).

59. *Video Privacy Protection Act*, ELEC. PRIV. INFO. CTR. [hereinafter VPPA EPIC], https://epic.org/privacy/vppa/ [https://perma.cc/HM87-5LM8].

60. *See* Solow-Niederman, *supra* note 12, at 619.

61. *See* R. Mark Halligan, *Pre-Filing Investigation of a Trade Secret Misappropriation Claim: The EONA Proofs*, REUTERS (Aug. 17, 2021, 1:15 PM), https://www.reuters.com/legal/legalindustry/pre-filing-investigation-trade-secret-misappropriation-claim-eona-proofs-2021-08-17/ [https://perma.cc/B6A9-UTSE] (noting that a plaintiff may bring suit under trade secret law and "prevail in a trade secret misappropriation lawsuit ... [by] submit[ting] evidentiary proof of existence, ownership, notice and access").

62. Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1).

63. *See, e.g.*, VPPA EPIC, *supra* note 59.

more modern forms of video consumption, such as streamed video feeds.[64]

Most states have adopted the *Second Restatement of Torts*' privacy law torts.[65] These torts include intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in a false light.[66] Each of these torts has a series of elements and operates as a quasi-property right—that is, they are rights to exclude from access or use of information that spring from a specific relational context between parties.[67]

Trade secret law gives owners of trade secrets a claim against those who wrongfully misappropriate protected information.[68] The

---

64. *See, e.g.*, Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 485, 489 (1st Cir. 2016). *But see* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015) (holding that downloading and using free mobile application does not make a user a "subscriber," therefore such a user cannot be a consumer under VPPA).

65. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1890 (2010) ("Courts readily embraced Prosser's formulation of privacy tort law. As the leading torts scholar of his time, Prosser was able to ensure that his interpretation of the privacy torts became the dominant one. In addition to being the most well-regarded torts scholar, Prosser was the leading treatise writer and casebook author. He was also the chief reporter for the *Second Restatement of Torts*, in which he codified his scheme for tort privacy. His influence encouraged courts and commentators to adopt his division of tort privacy into the four causes of action of intrusion, disclosure, false light, and appropriation. Even today, most courts look to the *Restatement*'s formulation of the privacy torts as the primary authority."); *see* RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977) (listing thirty-five states and District of Columbia that have expressly adopted the *Restatement* privacy torts).

66. RESTATEMENT (SECOND) OF TORTS § 652A-E (AM. L. INST. 1977).

67. Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1115-17, 1132 (2016).

68. *See, e.g.*, Robillard v. Opal Labs, Inc., 428 F. Supp. 3d 412, 451 (D. Or. 2019) ("To state a claim for misappropriation of trade secrets [under the Oregon Uniform Trade Secrets Act, plaintiff] must demonstrate that: (1) the subject of the claim qualifies as a statutory trade secret; (2) [plaintiff] employed reasonable measures to maintain the secrecy of its trade secrets; and (3) [defendant's] conduct constitutes statutory misappropriation."); WHIC LLC v. NextGen Lab'ys, Inc., 341 F. Supp. 3d 1147, 1162 (D. Haw. 2018) ("To prevail on a [claim under the Hawai'i Uniform Trade Secrets Act (HUTSA)], a plaintiff must establish that there exists a trade secret and a misappropriation of that trade secret."); Yeiser Rsch. & Dev. LLC v. Teknor Apex Co., 281 F. Supp. 3d 1021, 1043 (S.D. Cal. 2017) ("To plead a claim under the Delaware Uniform Trade Secrets Act ("DUTSA"), a plaintiff must allege that: (1) a trade secret existed; (2) the trade secret was communicated by the plaintiff to the defendant; (3) such communication occurred pursuant to an express or implied understanding that the secrecy of the matter would be respected; and (4) the trade secret was improperly used or disclosed by the defendant to the injury of the plaintiff.").

Uniform Trade Secrets Act, adopted by the vast majority of states,[69] defines a trade secret as:

> information, including a formula, pattern, compilation, program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[70]

Trade secret law, then, grants companies a right to keep certain valuable information private. The Defend Trade Secrets Act (DTSA), the federal trade secret law, proffers a substantially identical definition of trade secret and misappropriation thereof.[71]

Under a private enforcement regime, one individual sues another in court with a claim of right sounding in either statute or common law.[72] The right to sue also creates the potential for parties to negotiate out of court.[73] Most observers agree that the VPPA successfully protects privacy, although its scope is narrow.[74] Trade

---

69. *Trade Secret*, CORNELL LEGAL INFO. INST., https://www.law.cornell.edu/wex/trade_secret [https://perma.cc/P7NZ-V2DX].

70. UNIF. TRADE SECRETS ACT § 1(4) (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 1985), https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf [https://perma.cc/R6FD-EDF8].

71. Iacovacci v. Brevet Holdings, LLC, 437 F. Supp. 3d 367, 380 (S.D.N.Y. 2020) ("To state a claim for misappropriation under the DTSA, a plaintiff must allege that it possessed a trade secret that the defendant misappropriated. The elements for a misappropriation claim under New York law are fundamentally the same.... Since '[t]he requirements are similar,' courts have found that a '[c]omplaint sufficiently plead[ing] a DTSA claim ... also states a claim for misappropriation of trade secrets under New York law.'" (citations omitted)); Alta Devices, Inc. v. LG Elecs., Inc., 343 F. Supp. 3d 868, 877 (N.D. Cal. 2018) ("The elements of [trade secret] misappropriation under the DTSA are similar to those under the [California Uniform Trade Secrets Act], ... except that the DTSA applies only to misappropriations that occur or continue to occur on or after its date of enactment." (citation omitted)).

72. *See supra* notes 60-71 and accompanying text. While these particular statutes involve litigation, it is possible to have private enforcement without litigation in court. *See* Glover, *supra* note 23, at 1146-48.

73. *Cf.* Elizabeth Graham, *The Importance of a Mandatory Arbitration Carve-Out in a US Privacy Law*, IAPP (May 22, 2019), https://iapp.org/news/a/the-importance-of-a-mandatory-arbitration-carve-out-in-a-us-privacy-law/ [https://perma.cc/M4FK-SQJ6].

74. See *The Video Privacy Protection Act as a Model Intellectual Privacy Statute*, 131 HARV. L. REV. 1766, 1768-69 (2018) ("[T]he VPPA and recent cases deploying the Act suggest that courts are not hesitant to recognize privacy harms as 'injuries' when the harms implicate intellectual privacy. Because of its broad, technology-neutral language, the VPPA has

secret law covers a broad range of activity and successfully protects diverse interests of corporations.[75] By contrast, most commentators find the privacy law torts protecting consumer privacy to be ineffective.[76] What may account for this difference in effectiveness? One answer may be the superior ability of monied interests and repeat players to represent and defend their interests, but while this may be a salient issue, it is not unique to the protection of privacy.[77]

In the context of trade secret law, Sharon Sandeen persuasively argues that input from industry and practitioners in the development of a uniformly adopted state law of trade secret law distinguishes it from the four privacy torts, which are the brainchild of the reporter for the *Restatement of Torts*.[78] Yet, one main difference distinguishes general privacy law from trade secret law: ease of proof of harm.[79] Courts seem to have little trouble conceptualizing misappropriation of a trade secret as a harm.[80] In trade secret cases, the plaintiff usually has purely commercial rather than dignitary goals.[81] By contrast, in privacy cases, many courts have denied relief

---

managed to weather the past forty years. Though the statute's effectiveness, like that of any other statute, depends on reasonable judicial interpretation, the VPPA's resilience despite technological and doctrinal changes indicates that the statute might prove an appropriate model for the next logical step in safeguarding the privacy of expressive activity: federal reader privacy legislation."); Ann Stehling, Note, *From Blockbuster to Mobile Apps—Video Privacy Protection Act of 1988 Continues to Protect the Digital Citizen*, 70 SMU L. REV. 205, 210 (2017); VPPA EPIC, *supra* note 59 ("[The VPPA] stands as one of the strongest protections of consumer privacy against a specific form of data collection.").

75. *See, e.g.*, Abigail M. Luhn & Michael C. Zogby, *The Key to a Trade Secret Is Secrecy: Third Circuit Agrees Ownership Is Sufficient but Not Necessary to Maintain a Trade Secret Misappropriation Claim*, 10 NAT'L L. REV. (June 18, 2020); Ryan L. Marshall, Evi T. Christou & Theresa L. Starck, *From the Salon Chair to Court: L'Oréal Found Liable for Trade Secret Theft and Patent Infringement*, 9 NAT'L L. REV. (Sept. 3, 2019). Courts also readily find harm in right of publicity matters. White v. Samsung Elecs. Am., Inc., 971 F.2d 1395 (9th Cir. 1992); Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988); Alex Ben Block, *A Famed SoCal Soda Family Just Scored Big Bucks in a Case Against Coca-Cola*, L.A. MAG. (June 25, 2020), https://www.lamag.com/citythinkblog/hansens-soda-coca-cola-award/ [https://perma.cc/Q75L-YGMC].

76. *See, e.g.*, Solow-Niederman, *supra* note 12, at 614-18.

77. Marc Galanter, *Why the "Haves" Come out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95, 97-99, 103-04 (1974).

78. Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 681-92.

79. *See* Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361-62 (2014).

80. *See id.* at 363-64 (noting that "some jurists and scholars expect privacy harm to overcome" an (impossibly) high bar).

81. *See* Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543

to plaintiffs on the basis that there was no source of relief available to the plaintiff based on their inability to show harm.[82] Ryan Calo refers to courts' unique difficulty in finding harm in privacy intrusions as "privacy harm exceptionalism."[83] I have argued elsewhere that one way to improve private enforcement of privacy claims is to make restitutionary relief available to plaintiffs, that is, relief measured by defendant's gain rather than plaintiff's loss.[84]

Many federal courts employ procedural barriers to minimize access to justice for privacy invasions and dignitary harms more broadly.[85] Public enforcement of privacy matters can occur without being stymied by judicial skepticism of dignitary harms. Finally, even to the extent that private enforcement actions reach the court, there is the worry that private litigants or their lawyers will choose to advance their own private interests without consideration of the public interest in transparency of privacy disputes or deterring future wrongful conduct.[86] As a result, private enforcement without the support and legitimation of a public enforcer may struggle to be an ongoing source of deterrence for wrongdoers, as the common law privacy torts have.

C. Hybrid Enforcement Regimes

Hybrid enforcement regimes already exist in privacy law, and they have proven more effective than regimes that only use public enforcement. This Section describes and highlights the benefits of existing hybrid privacy regimes, distilling some general lessons for how to shape a hybrid enforcement regime for privacy laws.

The three most important examples of federal privacy statutes that have hybrid enforcement regimes are the Telephone Consumer Protection Act (TCPA),[87] the Fair Credit Reporting Act (FCRA),[88]

(2018).

82. *See* Calo, *supra* note 79, at 361-62.

83. *Id.*

84. Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653 (2019).

85. Rachel Bayefsky, *Remedies and Respect: Rethinking the Role of Federal Judicial Relief*, 109 GEO. L.J. 1263, 1270-73 (2021); Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 539-56 (2017).

86. *See* Eric Goldman, *The Irony of Privacy Class Action Litigation*, 10 J. ON TELECOMM. & HIGH TECH. L. 309, 314-15 (2012).

87. 47 U.S.C. § 227. TCPA regulates telemarketing practices, including prohibiting junk

and the Driver Privacy Protection Act (DPPA).[89] Edward Janger has observed that unlike the privacy torts, which are of a dignitary nature and seek primarily to compensate wronged individuals, these three laws "appear to be directed at using private parties as an adjunct to, or substitute for, public enforcement."[90] He noted that each of the private enforcement actions was constructed with awareness that "recovering actual personal damages is not going to be a sufficient incentive to bring suit."[91]

These laws have been largely successful in achieving concrete outcomes. TCPA limited abusive telemarketing practices, FCRA limited abuse of consumer credit files, and DPPA has effectively eliminated the use of drivers' records as a source of sensitive information. It is no accident they are all hybrid enforcement regimes.

These laws all protect individuals from privacy invasions that may in each individual instance be relatively small, but the laws reflect Congress's judgment that these invasions should not occur.

Public actors can act where small stakes and long odds may make individual action less likely. Public actors are well-suited for addressing collective problems because class actions with small claims are increasingly unlikely to pass muster,[92] so public avenues may be the better way to address collective problems. Furthermore, agencies can provide guidance and administer bright line rules,

---

faxes and certain types of automated calls. TCPA provides a private right of action. Individuals may sue for up to $500 for each violation or recover actual monetary loss, whichever is greater, and/or seek an injunction. In the event of a willful violation of the TCPA, a subscriber may sue for up to three times the damages.

88. 15 U.S.C. § 1681. FCRA regulates the collection, dissemination, and use of consumer information by credit agencies. FCRA provides a private right of action with actual, statutory, and punitive relief. Minimum statutory damages are $100, and actual damages are capped at $1,000, unless there was a "knowing" violation. The FCRA does not provide for equitable relief.

89. 18 U.S.C. § 2721. DPPA protects personal information collected by state motor vehicles departments from disclosure to other government officials and private parties. It creates a private right of action for knowing violations. The remedies available are substantial. The Act provides for payment of actual damages to the extent that they exceed $2,500, liquidated damages of $2,500 to the extent that the plaintiff is not able to prove greater damages, punitive damages for willful violations, an award of costs and reasonable attorney's fees, and equitable relief.

90. Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899, 907 (2003).

91. *Id.*

92. *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021).

such as the TCPA's Do-Not-Call Registry, administered by the Federal Communications Commission (FCC), and provide ongoing guidance to industry.

While there are many advantages to public enforcement, the reality is public enforcers cannot address every instance of wrongful telemarketing or use of consumer data for credit. Private rights of action allow every wrong under a statute to be a potential subject of litigation. Thus, private actors provide the primary incentive for companies to comply and agencies to continue to enforce these laws in every interaction with every consumer. Privacy invasions are personal, and private rights of action allow individuals to seek relief even if public actors do not have the resources or desire to pursue that claim. Public actors are often limited in their ability to pursue action, and even when they do, it can be difficult for them to actually collect monetary relief on their claim. In its enforcement of the TCPA, the FCC has issued hundreds of millions of dollars in fines for robocalls but has only collected on a fraction.[93] Private litigants are more likely to collect damages than a regulatory agency, which may make the threat of private suit more of a deterrent. While it is uncertain and potentially expensive to pursue a privacy claim, a small subset of dogged sticklers and their lawyers may decide to do so.[94] The potential of running into such a stickler encourages companies to follow the rules just as much as the threat of a regulatory fine. And given the limits of regulatory action in our country, the stickler plaintiff with her private right of action feels more likely, and more painful if it were to occur, than regulatory oversight. As one court put it, the threat of punitive damages from a private right of action for erroneous reporting under "the FCRA is the primary factor deterring erroneous reporting by the credit reporting industry."[95] A handful of plaintiffs and cases, then, provide the essential public good of creating case law that helps us

93. Sarah Krouse, *The FCC Has Fined Robocallers $208 Million. It's Collected $6,790.*, WALL ST. J. (Mar. 28, 2019, 7:00 AM), https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803 [https://perma.cc/N2W2-JFXT].

94. Yonathan A. Arbel & Roy Shapira, *Theory of the Nudnik: The Future of Consumer Activism and What We Can Do to Stop It*, 73 VAND. L. REV. 929, 931 (2020) (describing a "nudnik" as a particular type of fussy stickler consumer who forces companies to hold to their policies, and whose insistence has benefits to other, less litigious consumers).

95. Brim v. Midland Credit Mgmt., Inc., 795 F. Supp. 2d 1255, 1265 (N.D. Ala. 2011).

understand how the law applies to changing circumstances.[96] I say a handful simply because there are so many obstacles to succeeding on a privacy claim.[97] Yet even if few cases are brought, and fewer are successful, the benefits of a private right of action hold because of their deterrence function. The looming threat of individual action from individual consumers is essential for actually making sure companies are held accountable to privacy laws. Even unsuccessful individual cases can draw the agency's attention to problems. The public and private elements of a hybrid enforcement regime reinforce one another.

Legality shapes market and infrastructure practices. If the exercise of private rights of action incentivizes market actors to take privacy-enhancing behaviors by increasing the power of individuals to sanction non-privacy protective behavior, the reach of the law to protect privacy will extend further than if only public regulation is employed.[98] Several empirical studies have shown that "discovery can unearth otherwise-hidden information on corporate misconduct and lead to internal corporate reforms."[99] Discovery plays a key role in corporate law.[100] Joanna Schwartz observes that discovery forces firms to engage in "introspection" about their own practices and can lead to changes not mandated by judicial action or legal reform.[101] Information revealed during discovery can also influence public discussions about reform.[102]

---

96. *See* Samuel Issacharoff & Florencia Marotta-Wurgler, *The Hollowed Out Common Law*, 67 UCLA L. REV. 600, 600-01, 634-35 (2020) (describing the public good of case law and how electronic "contractual clauses compelling arbitration and forbidding claim aggregation" stifle the development of case law).

97. *See* Peter C. Ormerod, *Privacy Injuries and Article III Concreteness*, 48 FLA. ST. U. L. REV. 133, 133-35 (2020); Curtis R. Crooke, Comment, *Reply 'Stop' to Cancel: Whether Receiving One Unwanted Marketing Text Message Confers Standing in Federal Court*, 62 B.C. L. REV. E. SUPP. II.-84, II.-101 (2021).

98. *See* Justin H. Dion & Nicholas M. Smith, *Consumer Protection—Exploring Private Causes of Action for Victims of Data Breaches*, 41 W. NEW ENG. L. REV. 253, 257, 267, 275 (2019).

99. Diego A. Zambrano, *Discovery As Regulation*, 119 MICH. L. REV. 71, 75 n.13 (2020).

100. *See* Érica Gorga & Michael Halberstam, *Litigation Discovery and Corporate Governance: The Missing Story About the "Genius of American Corporate Law,"* 63 EMORY L.J. 1383, 1495-96 (2014).

101. Joanna C. Schwartz, *Introspection Through Litigation*, 90 NOTRE DAME L. REV. 1055, 1055 (2015).

102. *See* Gorga & Halberstam, *supra* note 100, at 1427, 1495-96.

In addition to providing access to the private sphere, private actions provide access to private expertise. Many of the relevant incidents happening in the private sphere—based in new, quickly evolving technical practices—outpace public actors' capabilities and complicate privacy regulation.[103] One of the reasons tendered for a lack of a federal omnibus privacy law is the lack of stable practices and public understanding of good policy in light of fast innovation, spawning fear of harming innovation in the service of protecting privacy.[104] To some extent, the portrayal of technology as simply too complex and difficult to regulate is a strategy to avoid regulation.[105] Yet, private enforcement is an essential tool for regulating technology.[106]

Private enforcement brings interactions in the private sphere to the surface for evaluation by public actors.[107] Without private enforcement, there is simply too much that is beyond the access and capability of the state's grasp.[108] The state does not understand

---

103. *See* Commonwealth v. Pitt, 29 Mass. L. Rptr. 445, 452 (Super. Ct. 2012) ("The development of technology has long outpaced the development of our laws."); *In re* Innovatio IP Ventures, LLC Pat. Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012) (order granting pretrial declaratory judgment) ("Any tension between that conclusion and the public's expectation of privacy is the product of the law's constant struggle to keep up with changing technology. Five or ten years ago, sniffing technology might have been more difficult to obtain, and the court's conclusion might have been different. But it is not the court's job to update the law to provide protection for consumers against ever changing technology. Only Congress, after balancing any competing policy interests, can play that role."); Felsher v. Univ. of Evansville, 755 N.E.2d 589, 591 (Ind. 2001) ("We live in an age when technology pushes us quickly ahead, and the law struggles to keep up. In this case, we encounter for the first time assumption of identity via the Internet. A number of existing statutes and common law precepts seem to serve surprisingly well in this dramatic new environment."); *see also* discussion of privacy problems *infra* Part III.

104. Schwartz, *supra* note 11, at 913 ("Thus, there was considerable caution in the United States in the 1970s against a broad regulation of information use that would include the private and public sectors in one fell swoop. This orientation demonstrates an ideology that I term 'regulatory parsimony.' As the medical profession expresses the idea, 'above all, do no harm.'").

105. *See, e.g.*, Kevin Maney, *The Law Can't Keep up with Technology ... and That's a Very Good Thing*, NEWSWEEK (Oct. 31, 2015, 2:27 PM), https://www.newsweek.com/government-gets-slower-tech-gets-faster-389073 [https://perma.cc/5Y94-7NVT] ("Speed to critical mass turns out to be a great strategy in the face of rickety laws and oblivious lawmakers. The faster companies move, the less government can get in their way.").

106. *See* Dion & Smith, *supra* note 98, at 257.

107. *See* ALEXANDRA LAHAV, IN PRAISE OF LITIGATION 57-58 (2017).

108. *See id.*

enough about new technosocial practices to immediately determine how best to regulate them.[109]

There is socioeconomic space and activity outside the sight of the state, which exists by design.[110] Denying the state access to societal space, which I will call a "private sphere," without express permission has many civil rights benefits in a liberal society.[111] However, if the government cannot access the private sphere, it also cannot directly regulate wrongs that occur there. Some privacy violations are unlikely to be directly observed by the state, which makes private enforcement an essential tool for learning about these wrongs.

When I refer to a private sphere free from government surveillance and intervention, I mean that in two ways. First, I mean spaces and resources that government cannot access or observe.[112] An example of this is a locked analog safe containing analog items on private property. Second, I mean spaces, information, and resources that may be visible to anyone but only interpretable by people with either proprietary interpretative tools, or highly specialized skills that only high-demand, highly compensated people in private industry tend to have.[113] This makes government access impossible or highly unlikely, respectively, without private collaboration or a court order.[114] Examples of this latter type of private

---

109. *See* Commonwealth v. Pitt, 29 Mass. L. Rptr. 445, 452 (Super. Ct. 2012); Alex Engler, *What All Policy Analysts Need to Know About Data Science*, BROOKINGS (Apr. 20, 2020), https://www.brookings.edu/research/what-all-policy-analysts-need-to-know-about-data-science/ [https://perma.cc/9FHY-FS9F].

110. *See* Dagan & Dorfman, *supra* note 12, at 1416-17.

111. *See, e.g.*, Louise Marie Roth, *The Right to Privacy Is Political: Power, the Boundary Between Public and Private, and Sexual Harassment*, 24 LAW & SOC. INQUIRY 45, 45-46 (1999). The precise scope of the private sphere is a contested concept in the literature. G. Alex Sinha, *A Real-Property Model of Privacy*, 68 DEPAUL L. REV. 567, 572 (2019). Some contest the usefulness of a notion of a private sphere in privacy law at all. *E.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1131-32 (2002) (observing that "the metaphor of space has significant limitations," and that "[w]e can avoid allowing the metaphor of space to limit our understanding of privacy"). The skepticism of a private sphere parasites on the assumption of a pre-political private law that lacks rule of law considerations. *See* discussion *infra* Part III.E.

112. *See* Roth, *supra* note 111, at 57-58 (arguing that the ability of the government to surveil divides the private and public spheres).

113. *See* Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-By-Design*, 106 CALIF. L. REV. 697, 702 (2018).

114. *See id.* Some argue that collaborative governance is a way to bring private sector expertise into governance. *E.g.*, Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 76 (1997). Collaborative governance is defined as "[a]

sphere include an algorithm with public outputs, such as a search engine, a high-speed trading software, or an internet of things (IoT) smart product.[115] While all can see the algorithm's designated output, individuals outside of the firm would face significant difficulties evaluating the algorithm's sources and determining whether its output reflects illegal or immoral intent on the part of its creators.[116]

In both senses, the private sphere is particularly important to the regulation of privacy. Access to the private sphere is a prerequisite for addressing many privacy wrongs. Many invasions of privacy occur in private, where no outside party can observe what is happening in order to contest its wrongfulness;[117] for example, a wrongful sale of consumer information between private parties. Expertise barriers are also salient in the area of privacy.[118] Many novel data protection deficiencies and methods of digital market manipulation are too complicated for regulators to readily understand.[119] Civil litigation brings practices to light that regulators may not even know to look for.[120] What is more, translation through

---

governing arrangement where one or more public agencies directly engage non-state stakeholders in a collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets." Chris Ansell & Alison Gash, *Collaborative Governance in Theory and Practice*, 18 J. PUB. ADMIN. RSCH. & THEORY 543, 544 (2008). While expertise of this type is valuable, it is of a different character from expertise brought to bear on a specific dispute. LAHAV, *supra* note 107, at 56-61 (discussing the information value of litigation). The context of a dispute also changes the way information is presented and analyzed in a way that is more useful for democracy. *Id.* at 58 ("[L]itigation can combine the facts and the law to produce narratives and provide explanations for why past events occurred, frameworks for addressing hurtful incidents, and opportunities for healing as a result."). Furthermore, "in political discourse people can rely on misrepresentations, speculations, and hyperbole, but a trial is exacting and challenges such assertions." *Id.* at 66.

115. *See generally* Tam Harbert, *Practical Uses of the Internet of Things in Government Are Everywhere*, GOV'T TECH. (Jan. 3, 2017), https://www.govtech.com/network/practical-uses-of-the-internet-of-things-in-government-are-everywhere.html [https://perma.cc/VL96-ZYC7] (identifying the lack of understanding in government of IoT data outputs as a barrier to implementation of progressive technologies).

116. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 718, 725 (2016).

117. *See, e.g.*, Roth, *supra* 111, at 63-67.

118. *See* Engler, *supra* note 109.

119. *See id.*

120. *See* LAHAV, *supra* note 107, at 57-58; *see also* Elizabeth Chamblee Burch & Alexandra D. Lahav, *Information for the Common Good in Mass Torts*, 70 DEPAUL L. REV. 345, 353-360 (2021) (describing examples of how transparency in tort litigation informed the public and regulators of hitertho unknown or poorly understood hazardous products and practices).

analogy of specialist information into generalist terms is the particular virtue of judges.[121] It is important that these issues become cognizable to the public so that norms can emerge about what behavior is wrongful.

Private enforcement's acute information-forcing and diagnostic analytical properties are necessary to undergird public law regulations.[122] Many of the fact patterns and technical knowledge lawmakers need in order to regulate privacy are ensconced deep within the private sphere, and we need robust private enforcement of privacy law to flush them out.[123]

The scope and resources of public enforcement paired with the potential for uncompromising, stickler private plaintiffs to insist on enforcing the law leads to ongoing, thoughtful enforcement of privacy law. Comparing the hybrid enforcement of privacy laws to purely public and purely private enforcement illustrates the wisdom of including both elements. Private enforcement has an important role to play in regulating newly possible, poorly understood phenomena because it allows for broad, resilient, innovative enforcement.[124]

---

121. *See* Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 767-68, 784, 787 (1993).

122. *See* Tun-Jen Chiang, *The Information-Forcing Dilemma in Damages Law*, 59 WM. & MARY L. REV. 81, 91-92 (2017) (discussing how, in litigation, burdens of proof serve as an "information-forcing mechanism," and that without such burdens, courts would have no framework for acquiring evidence or making decisions); Alex Reinert, *Pleading as Information-Forcing*, 75 LAW & CONTEMP. PROBS. 1, 29-30 (2012) ("The classic justification for information-forcing rules, stemming from Ayres and Gertner's analysis of contract law, is that they provide an incentive for the party with the best access to private information to disclose it to a contracting party or third parties. These information-forcing rules are meant, among other things, to decrease transaction costs for third parties." (footnotes omitted)).

123. *See* Zambrano, *supra* note 99, at 75 n.13. There is well-developed literature on the use of default rules in contract law to force knowledgeable parties to share information relevant for claims and regulation. *E.g.*, J.H. Verkerke, *Legal Ignorance and Information-Forcing Rules*, 56 WM. & MARY L. REV. 899, 904 (2015); Eric Maskin, *On the Rationale for Penalty Default Rules*, 33 FLA. ST. U. L. REV. 557 (2006); Barry E. Adler, *The Questionable Ascent of* Hadley v. Baxendale, 51 STAN. L. REV. 1547, 1580-81 (1999); Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 97 (1989) (arguing that "penalty default" rules in contract law incentivize disclosure).

124. *Cf.* Maureen L. Condic & Samuel B. Condic, *The Appropriate Limits of Science in the Formation of Public Policy*, 17 NOTRE DAME J.L. ETHICS & PUB. POL'Y 157, 177 (2003) (affirming limits of scientific expertise for answering moral and political questions).

Private enforcement can be "a dramatically effective source of deterrence."[125] Accountability and deterrence are sorely needed in the privacy space. The struggles of the FTC in this space show that public enforcement has not proven an adequate check on unfair and deceptive privacy practices. A generic concern about private enforcement is overdeterrence,[126] but when considering private rights of action it is important to consider the cause of action proposed and the specific regulatory context. Support for public enforcement is essential to ensure any real accountability for firms. A limited private right of action, for example a right to an explanation for an algorithm's output, can serve many of the information forcing and deterrence functions extolled here. As Bruce Klaw has observed in the context of Federal Corrupt Practices Act private enforcement, "criminological research shows that *likelihood* of detection and subsequent sanction, rather than *severity* of sanction is the key determinant to deterrence."[127] Private rights of action need not be broad with extreme penalties to serve the functions of deterrence and additional regulatory coverage. Tailoring the private right of action through statutory framing or administrative guidance can influence the amount of private enforcement to attain the desired amount of deterrence.[128]

II. DIGNITY AND PRIVATE ENFORCEMENT

Private rights of action accord individuals the power to enforce their own rights, thereby affirming the dignitary status of

125. Bruce W. Klaw, *A New Strategy for Preventing Bribery and Extortion in International Business Transactions*, 49 HARV. J. ON LEGIS. 303, 359 (2012).

126. Matthew C. Stephenson, *Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies*, 91 VA. L. REV. 93, 114 (2005) ("[P]rivate rights of action can lead to inefficiently high levels of enforcement, causing waste of judicial resources and leading to excessive deterrence of socially beneficial activity.").

127. Klaw, *supra* note 125, at 360.

128. FARHANG, *supra* note 28, at 21-31 (describing ways legislatures can exercise control over the amount of private litigation arising from a private right of action); *see also* Stephenson, *supra* note 126, at 95-96, 121-43 (arguing executive agencies should play an enhanced role in shaping private enforcement policy).

citizens.[129] This Part contributes a framework for understanding private enforcement of privacy rights as essential.[130]

Private rights of action uniquely speak to the dignity of the citizen by putting power to contest wrongs in her hands and allowing the individual to construct claims as entitlements.[131] Each of these specific implications is of particular importance in privacy regulation.

Private enforcement is significant for citizen engagement and identity.[132] Private enforcement takes the form of a suit brought by one member of society against another, making a claim or right.[133] The right to bring suit has meaning, and the reasonable expectation of the plaintiff's success accentuates that right.[134] Private law in its individual-to-individual, confrontational form speaks to the dignity and power of each citizen,[135] as its origins as the sole source of rights for English citizens suggests.[136] Individuals attach greater value to rights they possess versus interests provided at the sovereign's leisure.[137]

---

129. *See, e.g.*, Anuradha Joshi, *Legal Empowerment and Social Accountability: Complementary Strategies Toward Rights-Based Development in Health?*, 99 WORLD DEV. 160, 160-61 (2017).

130. *See* James J. Park, *Rules, Principles, and the Competition to Enforce the Securities Laws*, 100 CALIF. L. REV. 115, 120 (2012).

131. *See* Dagan & Dorfman, *supra* note 12, at 1416.

132. *Id.* at 1416-17.

133. *See generally* Shyamkrishna Balganesh, *Private Law Statutory Interpretation*, 92 S. CAL. L. REV. 949, 949 (2019) (defining private law as horizontal interactions between members of society).

134. *See, e.g.*, Dagan & Dorfman, *supra* note 12, at 1416-22.

135. *See* Ori J. Herstein, *How Tort Law Empowers*, 65 U. TORONTO L.J. 99, 109 (2015) ("Th[e] power to expose others to the power of courts is, of course, a general feature of civil litigation, which is not restrictive to the context of tort victims and tortfeasors, but mostly available to all would-be plaintiffs."); Nathan B. Oman, *The Honor of Private Law*, 80 FORDHAM L. REV. 31, 32 (2011) (defending civil recourse as a way of vindicating one's honor); Jason M. Solomon, *Civil Recourse as Social Equality*, 39 FLA. ST. U. L. REV. 243, 259-62 (2011) (defending civil recourse as a way of maintaining social equality); Benjamin C. Zipursky, *Substantive Standing, Civil Recourse, and Corrective Justice*, 39 FLA. ST. U. L. REV. 299, 327, 336, 338 (2011) (defending civil recourse as means of self-restoration); *see also* Matthew A. Shapiro, *Civil Wrongs and Civil Procedure*, *in* CIVIL WRONGS AND JUSTICE IN PRIVATE LAW 87, 93-94 (Paul B. Miller & John Oberdiek eds., 2020); ARTHUR RIPSTEIN, PRIVATE WRONGS 271-72 (2016) (analyzing property and contract in terms of civil recourse).

136. Ariel Katz, *Intellectual Property, Antitrust, and the Rule of Law: Between Private Power and State Power*, 17 THEORETICAL INQUIRIES L. 633, 650 (2016).

137. *Cf.* Richard Thaler, *Toward a Positive Theory of Consumer Choice*, 1 J. ECON. BEHAV. & ORG. 39, 44 (1980) (defining "endowment effect" as the phenomenon of people demanding

As Hanoch Dagan and Avihay Dorfman put it:

> Since private law is the law of our horizontal interactions, its roles cannot be properly performed by any other legal field. Only private law can forge and sustain the variety of frameworks for interdependent interpersonal relationships that allow us to form and lead the conception of our lives. Only private law can cast these frameworks of relationships as interactions between free and equal individuals who respect each other for the persons they actually are and thereby vindicate our claims to relational justice from one another.[138]

The form of private enforcement speaks to its unique function in a liberal society: it is not merely an incidental form of regulation, but a statement about the status of each person in our society.[139]

The person, as a rights-bearer, is particularly important in privacy law.[140] Some authors contend that ongoing relationships of trust between information-age firms and customers—in which opportunism, incentives, and options abound for the firm—create fiduciary duties to customers.[141] The reconceptualization of the citizen in the information age as an agent with powers, rather than just a passive user, would have important social consequences.[142] There has been much ink spilled on the problem of data protection exhaustion, the concept that citizens resign to having their data exploited as an inevitable consequence of existing in society.[143] A

---

more to give up an object they own than they would be willing to pay to acquire it).

138. Dagan & Dorfman, *supra* note 12, at 1398.

139. *See id.*

140. *See id.* at 1397-98.

141. *E.g.*, Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 144, 158-59 (2020).

142. *Cf.* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/ZN4M-546N] (describing the negative consequences of depriving individuals of privacy rights in the information age).

143. *See, e.g.*, Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman & Susanne Furman, *Security Fatigue*, 18 IT PRO. 26, 26 (2016); Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/76KJ-4SAX] ("A majority of Americans believe their online and offline activities are being tracked

private enforcement regime to give citizens meaningful options to contest data practices has benefits beyond altering the law. After all, many citizens lack the time or resources to pursue data protection claims, and if they do their efforts may not be successful.[144] The expressive function of private enforcement increases individuals' belief in their own agency as members of society and rights-bearers.[145] Bolstering that sense of agency is important in the internet age—with respect to privacy in particular—because of its connection to the preconditions of liberal democracy.[146] Through technology, small claims litigation may be made easier and cheaper for claimants.[147]

Private rights of action avoid the problem of under-enforcement by an administrative agency leading to the nonenforcement of a right.[148] Privacy invasions, like other torts, are too socially pervasive for one or even multiple administrative authorities to satisfactorily identify, investigate, and adjudicate in all instances.[149]

---

and monitored by companies and the government with some regularity. It is such a common condition of modern life that roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life *without having data collected about them* by companies or the government.").

144. *See* Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal US Privacy Litigation*, IAPP (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/ [https://perma.cc/V7YP-XDS3] (identifying court costs and minimal available damages under existing and prospective rights of action as dissuading factors for bringing a privacy suit).

145. *See* Herstein, *supra* note 135, at 101.

146. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 11 (2015) ("[P]rivacy [is] necessary to produce speech ... privacy has three essential elements—freedom of thought, the right to read freely, and the right to communicate in confidence.").

147. *See generally* Matt Byrne, *Global Litigation 50: Does Legal Tech = Lower Litigation Fees, and Other Tech Dilemmas*, THE LAW. (Sept. 4, 2017, 8:00 AM), https://www.thelawyer.com/legal-technology-litigation-law-firms-top-50/ [https://perma.cc/4XW8-LU7C] (describing the development of "largely tech-driven methods of litigating," which will "deliver projects more quickly and cheaply"); Janet Walker & Garry D. Watson, *New Trends in Procedural Law: New Technologies and the Civil Litigation Process*, 31 HASTINGS INT'L & COMPAR. L. REV. 251, 286 (2008) (positing that technological advances will "[m]ak[e] the civil justice system more accessible" and less expensive for the majority of Americans); Richard M. Re & Alicia Solow-Niederman, *Developing Artificially Intelligent Justice*, 22 STAN. TECH. L. REV. 242, 255-56 (2019) ("But for any given level of technically attainable accuracy, use of AI adjudication would lower costs.").

148. *See* Clopton, *supra* note 22, at 295-308.

149. *Cf.* Robert L. Rabin, *Poking Holes in the Fabric of Tort: A Comment*, 56 DEPAUL L. REV. 293, 303 (2007) (explaining how administrative agencies cannot adequately monitor the

This Part's analysis leads to some broader conclusions for privacy advocates beyond simply the import of private rights of action in privacy legislation. In order for the benefits rehearsed here to accrue, there must be a practical means for individuals to bring cases.[150] There are legal and practical barriers to bringing privacy lawsuits. To make private rights of action for privacy rights effective, the surrounding regime must support them.

The two principal legal barriers keeping privacy matters out of court are elevated harm requirements for privacy matters,[151] and mandatory arbitration clauses in consumer contracts.[152] Courts are often hesitant to deliver distributive justice if legislatures have been silent or ambivalent on an issue.[153] Yet, if state legislatures and Congress take decisive action on privacy, that worry will dissipate.[154] Judges could move away from interpretations that keep privacy matters out of court.[155] Clear legislative instructions could also spur courts along this path.[156]

The practical barrier to privacy lawsuits comes, of course, at the expense of plaintiffs.[157] Awarding attorney's fees for successful plaintiffs, as is allowed by the Magnusson-Moss Warranty Act, could ameliorate this barrier.[158]

The next Part applies this general framework to individual privacy problems of the day to illustrate its relevance.

---

countless incidents of consumer misuse of products).

150. *Cf.* Kerry, *supra* note 142 (arguing that the lack of a practical means for individuals to bring privacy suits degrades individual rights).

151. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022).

152. *See* Graham, *supra* note 73.

153. *See* William N. Eskridge, Jr., *Interpreting Legislative Inaction*, 87 MICH. L. REV. 67, 67 (1988).

154. *But see* Citron & Solove, *supra* note 151.

155. *But see id.*

156. *See* Jennifer Bryant, *2021 'Best Chance' for US Privacy Legislation*, IAPP (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ [https://perma.cc/U9KK-JWKX].

157. Dayton Uttinger, *How Much Does It Cost to File a Civil Suit and When Should You?*, FISCAL TIGER (Jan. 18, 2018), https://www.fiscaltiger.com/how-much-does-it-cost-file-civil-suit/ [https://perma.cc/Z4QL-PFYN].

158. *See* Magnuson-Moss Warranty Act, 15 U.S.C. § 2310(d)(2).

III. PRIVATE ENFORCEMENT AND MODERN PRIVACY PROBLEMS

This Part addresses a suite of privacy issues in the modern information ecosystem. Showing how private enforcement can help address the major privacy problems of the day makes concrete the two independent justifications of Parts I and II: deterrence and citizen dignity, respectively.[159] For each privacy issue, I outline the problem, evaluate the deterrence and dignity benefits of private enforcement, and discuss sector-specific challenges. The discussion of private enforcement's role in regulating these privacy problems is intentionally cursory. The point is to model how the general justifications for private enforcement map onto addressing specific privacy problems.

A. Nonconsensual Pornography

Nonconsensual pornography, sometimes called revenge pornography, is the distribution of pornographic images of a person without their approval.[160] The distributor intends to humiliate and harm the victim.[161] Technological innovation facilitates this type of wrong.[162] While individuals may have wished to embarrass others by distributing such images prior to the information age, the ability to publicly distribute and alter images and videos with ease has only been possible since the early 2000s.[163] Victims of nonconsensual

159. *See* discussion *supra* Parts I-II.

160. Yanet Ruvalcaba & Asia A. Eaton, *Nonconsensual Pornography Among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men*, 10 PSYCH. VIOLENCE 68, 68 (2020) ("Though the media has often used the term *revenge porn* to describe nonconsensual pornography, there are important distinctions between those two terms. First, revenge porn implies the dissemination of images for the purpose of humiliating or harming the victim. Nonconsensual pornography, however, is not always motivated by revenge. Second, the term revenge porn implies that the victim instigated the harm by doing something for which the perpetrator is seeking revenge, supporting rape myths that blame victims for their own abuse. For these reasons, and others, scholars and advocates tend not to use the term revenge porn." (citations omitted)).

161. *Id.*

162. *Id.*

163. *See* Karolina Mania, *The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective*, 24 SEXUALITY & CULTURE 2079, 2082 (2020) (providing a historical background of key moments in nonconsensual pornography, including an early example of reader photos accepted and published by *Hustler* in the early 1980s, some

pornography may be psychologically damaged and exposed to personal and professional losses.[164] Women are disproportionately impacted by this type of wrong.[165] Nonconsensual pornography is the most prominent of a family of practices that expose and commodify the naked bodies and intimate details of people.[166]

Although there is no federal statute on this topic,[167] the vast majority of states have criminalized nonconsensual pornography, and many have also created civil private rights of action for victims.[168] In 2013, only three states criminalized nonconsensual pornography.[169] As of January 2022, forty-eight states and the District of Columbia have nonconsensual pornography laws.[170] In 2018, the Uniform Law Commission (ULC) approved the Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act—model legislation that establishes civil remedies for victims of nonconsensual pornography, and "[a]bout a dozen state laws currently allow for a private right of action against those who disclose

---

of which turned out to have been submitted without the consent of the photo's subject).

164. Benjamin Powers, *Revenge Porn Can Haunt You for Years*, TEEN VOGUE (Aug. 26, 2019), https://www.teenvogue.com/story/cost-of-revenge-porn [https://perma.cc/N5E6-LMGS].

165. Lindsay Holcomb, *The Role of Torts in the Fight Against Nonconsensual Pornography*, 27 CARDOZO J. EQUAL RTS. & SOC. JUST. 261, 267 (2021) ("Ninety-three percent of the victims of nonconsensual porn are female, and images of women make up the vast majority of content posted on websites dedicated to nonconsensual pornography. Men are twice as likely to have shared nonconsensual porn than women, and women are 2.5 times as likely to have been threatened with nonconsensual porn.... Finally, nonconsensual porn is perpetrated against sexual minorities at rates slightly higher than against individuals who identify as heterosexual." (footnotes omitted)).

166. *See* Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1783 (2021).

167. A federal bill has been proposed, but it has not been passed. *See* Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong.

168. Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1269 (2017); *see also* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

169. *See* Franks, *supra* note 168, at 1255.

170. *See 48 States + DC + Two Territories Now Have Laws Against Nonconsensual Pornography*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/nonconsensual-pornagraphy-laws/ [https://perma.cc/25JN-6V9B]; *AG FITCH: Criminalizing Revenge Porn Gives Victims Hope, Dignity, and a Better Future*, Y'ALL POL. (May 20, 2021), https://yallpolitics.com/2021/05/20/ag-fitch-criminalizing-revenge-porn-gives-victims-hope-dignity-and-a-better-future/ [https://perma.cc/87XK-A5WZ] ("On April 16, 2021, Governor Reeves signed into law S.B. 2121, ... criminalizing 'revenge porn' and protecting innocent people from repeated victimization."). Two states—South Carolina and Massachusetts—have proposed legislation. *See* Revenge Porn Act, S. 567, 123d Sess. (S.C. 2019); H.R. 76, 191st Sess. (Mass. 2019).

intimate images without consent."[171] The ULC underscored the importance of a private right of action in the Act's preamble: "[w]hile criminal law can serve as an important deterrent and expression of social condemnation, civil law is better suited to compensate victims for the harm they have suffered." Civil law allows victims to use the lower "preponderance of the evidence" standard inherent in civil cases to receive relief. Furthermore, victims can receive compensatory damages for mental distress and reputational harm from the wrong.[172] More broadly, enabling victims to sue empowers the victims and allows them to take their fate into their own hands.[173] Given the personal consequences and dignitary harm a victim of nonconsensual pornography faces, it seems unjust to allow whether the perpetrator sees justice to come down to whether an overburdened or unwilling prosecutor sees fit to take the case.[174]

State nonconsensual pornography laws can target not only individuals who post nonconsensual pornography, but also—with more difficulty—websites and platforms that host nonconsensual pornography.[175] Section 230 of the Communications Decency Act generally shields website hosts and providers from liability,[176] but websites that actively encourage the behavior may be liable for nonconsensual pornography distribution.[177] The flurry of legislation

171. Pam Greenberg, *Fighting Revenge Porn and 'Sextortion,'* LEGISBRIEF (Aug. 2019), https://www.ncsl.org/Portals/1/Documents/legisbriefs/2019/AugustLBs/Revenge-Porn-and-Sextortion_29.pdf [https://perma.cc/JH3C-8UD7]; *see also Civil Remedies for Unauthorized Disclosure of Intimate Images Act*, UNIF. L. COMM'N, https://www.uniformlaws.org/committees/community-home?CommunityKey=668f6afa-f7b5-444b-9f0a-6873fb617ebb [https://perma.cc/RRB6-EK2K] (reporting that six states—Arkansas, Iowa, South Dakota, Nebraska, Colorado, and West Virginia—have enacted the model legislation, and two states—Missouri and Arizona—have introduced such bills).

172. Jayne S. Ressler, *Anonymous Plaintiffs and Sexual Misconduct*, 50 SETON HALL L. REV. 955, 968-70 (2020).

173. *Id.*; *see also* Lesley Wexler, Jennifer K. Robbennolt & Colleen Murphy, *#MeToo, Time's Up, and Theories of Justice*, 2019 U. ILL. L. REV. 45, 76-78 (describing the role money damages can play in psychologically making victims whole).

174. Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1879-81 (2019).

175. *See* Franks, *supra* note 168, at 1286-95 (describing the characteristics of state statutes with examples).

176. 47 U.S.C. § 230.

177. Karla Utset, Note, *Drawing the Line: The Jurisprudence of Non-Consensual Pornography and the Implications of Kanye West's* Famous *Music Video*, 72 U. MIA. L. REV. 920, 928 (2018) ("[C]ourts interpreting Section 230 sharply distinguish between ISPs 'who simply host third-party content and those who actively participate in the creation of illegal

on nonconsensual pornography has led to changes in business practices outside the courtroom. These laws have led many platforms to revise their terms of service to prohibit nonconsensual pornography and to filter such content, notwithstanding the protection that section 230 provides platforms.[178]

The widespread adoption of nonconsensual pornography legislation is one of the law's greatest expansions of the privacy interest in recent years. States recognized an important privacy interest and reinforced existing law to better protect it. Sexual privacy, although it has its own unique characteristics,[179] is undoubtedly among the interests protected in the general genus of privacy.[180] State legislation started out focused on criminalizing nonconsensual pornography, yet that has given way to a more recent trend of having civil private rights of action as well. The near-universal criminalization of nonconsensual pornography has given way to understanding nonconsensual pornography as a civil wrong as well. What's more, courts have declined to strike down nonconsensual pornography laws on First Amendment grounds.[181] Nonconsensual pornography is an area of privacy law that has a clear positive trend.

---

content.'" (quoting Andrew McDiarmid, *Decisive Section 230 Victory for GoDaddy in Revenge Porn Case*, CDT: BLOG (Apr. 15, 2014), https://cdt.org/blog/decisive-section-230-victory-for-godaddy-in-revenge-porn-case/)).

178. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1764-65 (2019) ("For instance, content platforms have terms-of-service agreements, which ban certain forms of content based on companies' values. They experience pressure from, or adhere to legal mandates of, governments to block or filter certain information like hate speech or 'fake news.'" (footnotes omitted)); Franks, *supra* note 168, at 1278 ("In January 2015, the Federal Trade Commission (FTC) issued a complaint and a proposed consent order against Craig Brittain, the owner of the (now defunct) revenge porn site Is Anybody Down. The complaint alleged that Brittain engaged in unlawful business practices by obtaining sexually explicit material of women through misrepresentation and deceit and disseminating this material for profit. According to the terms of the settlement, Brittain must destroy all such material and is barred from distributing such material in the future without the 'affirmative express consent in writing' of the individuals depicted. In doing so, the FTC effectively declared the business model of revenge porn sites to be unlawful—a tremendous vindication for the victims of nonconsensual pornography." (footnotes omitted)).

179. *See generally* Citron, *supra* note 174.

180. *See* Roni Rosenberg & Hadar Dancig-Rosenberg, *Reconceptualizing Revenge Porn*, 63 ARIZ. L. REV. 199, 218-20 (2021) (arguing that nonconsensual pornography should be conceptualized as a sex offense, and not merely a privacy offense, but conceding that nonconsensual pornography is a privacy violation).

181. *See, e.g.*, People v. Austin, 155 N.E.3d 439, 466, 472 (Ill. 2019), *cert. denied*, 141 S. Ct. 233 (2020).

Yet, privacy literature rarely highlights the success of nonconsensual pornography legislation as a model for future effective privacy legislation. There are several possible reasons for this.[182] I will focus on the two most likely. First, privacy scholarship has a near-unanimous skepticism of sectoral legislation.[183] Legislators cannot anticipate all the forms privacy problems may take or even the sectors that will be most important to regulate. So, one may not look to nonconsensual pornography legislation as a blueprint because of concerns about its limited scope. Second, nonconsensual pornography is somewhat exceptional among privacy interests insofar as its visceral immediacy. Privacy law, in general, is plagued by the perception that privacy harms are based on subjective personal preferences.[184] By contrast, there is deep-seated American cultural conservatism around nudity and sexual privacy.[185] Thus, it proved easy to build political consensus around the need to protect this particular privacy interest, but there is skepticism that the path nonconsensual pornography legislation took could be followed by other privacy interests or a more general privacy interest.[186] Yet, recent conversations about privacy have revealed that consensus on a more general right of privacy is possible. While only three

182. One, unfortunately, may be the tendency for scholarship not squarely addressing gender to ignore scholarship focusing on issues that predominately impact women. *See* Christopher A. Cotropia & Lee Petherbridge, *Gender Disparity in Law Review Citation Rates*, 59 WM. & MARY L. REV. 771, 777 (2018). Furthermore, women write most of the scholarship on nonconsensual pornography, and there is a proven bias in academia against citing articles by authors with female names. *Id.* at 771; *cf.* Katherine A. Mitchell, *The Privacy Hierarchy: A Comparative Analysis of the Intimate Privacy Protection Act vs. the Geolocational Privacy and Surveillance Act*, 73 U. MIA. L. REV. 569, 614 (2019) ("With the advent of legislative reform in the United States protecting women's rights, the criminal legal landscape has dramatically changed. Yet, our country is still plagued by a lack of recognition for women's rights to sexual, physical, and expressive autonomy—a fundamental flaw underlining the reason why there may be a societal lack of empathy for victims of nonconsensual pornography.").

183. *See, e.g.*, BJ Ard, *The Limits of Industry-Specific Privacy Law*, 51 IDAHO L. REV. 607 (2015).

184. Will Rinehart, *What Exactly Constitutes a Privacy Harm?*, AM. ACTION F. (June 1, 2016), https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/ [https://perma.cc/QQH2-PH68].

185. *See* Franks, *supra* note 168, at 1260 (discussing how there are generally negative perceptions about nudity and displays of sexual conduct).

186. *But see* Mitchell, *supra* note 182, at 572 (arguing that it is difficult to get nonconsensual pornography legislation passed relative to more gender-neutral Geolocational Privacy and Surveillance (GPS) legislation).

states have passed privacy legislation, the majority of states are seriously exploring the prospect.[187] What is stymieing legislation from passing is not a lack of agreement on whether there is a general privacy right but on how effective enforcement of that right should be.[188] So the path of nonconsensual pornography in statehouses is instructive and encouraging for a more general privacy right at the state level.

Nonconsensual pornography legislation offers valuable lessons about the form privacy law should take if it is to succeed in protecting a privacy interest.[189] An emphasis on private rights of action could further deter and prevent distribution of nonconsensual pornography. Of course, the rights of action further the interests of the victims, but having a civil action for individuals does more than this. One small claims case could draw attention to an issue with a platform. Private enforcement creates an additional avenue for society to have conversations about sexual misconduct.

Most significantly, the dignitary aspect of this wrong is predominant. Whether a victim of this abuse is able to seek relief should at least potentially come down to her choice, not the whim of a public servant. To the extent that there is conflict between deterrence and civil recourse goals of private enforcement, civil recourse should carry the day. Yet deterrence separately strongly calls for private enforcement, given the public interest in avoiding these wrongs from occurring in the first place.

B. Data Insecurity

The interconnectedness of devices via the internet has made information exponentially more vulnerable to theft and misappropriation.[190] This includes highly sensitive information, such as medical information collected in real time from the body[191] and physical

187. Klosowski, *supra* note 35.

188. *Id.*

189. *See generally* Mitchell, *supra* note 182, at 606 (noting the overlapping areas that other privacy issues have with nonconsensual pornography).

190. Max Meglio, Note, *Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation*, 61 B.C. L. REV. 1223, 1247-48 (2020).

191. *See* Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WM. & MARY L. REV. 77, 81-86 (2019).

location data.[192] Protecting data necessarily involves tradeoffs. For example, effective network security is often expensive and can diminish user experience.[193] Moreover, because network intrusions are considered inevitable, industry has focused on cyber resiliency—managing risk and mitigating the impact of intrusions.[194] Companies weigh the costs of additional cybersecurity measures against the potential costs of an intrusion.[195] As a result, many companies that offer consumer-facing devices, platforms, and databases underinvest in cybersecurity measures because of the low cost of consumer cybersecurity failures. Although data breach disclosure laws require companies to disclose data breaches impacting consumers, the lack of a private right of action insulates companies from the costs associated with data breaches that compromise consumer data.[196] Under the status quo, companies are able to allow their users to absorb the costs of data breach failures because opportunities for seeking direct compensation for data breaches are highly limited.

Many highly publicized hacks of large consumer databases have exposed many people's personal data.[197] Victims of such hacks could

192. *See generally* Meglio, *supra* note 190, at 1250 (discussing how consumers often are too willing to trade personal data at the expense of privacy and security).

193. *See* Steve Morgan, *Global Cybersecurity Spending Predicted to Exceed $1 Trillion from 2017-2021*, CYBERCRIME MAG. (June 10, 2019), https://cybersecurityventures.com/cyber security-market-report/ [https://perma.cc/UNW9-EH4F]; James Brown, *The Art of Balancing User Experience and Security*, USABILITY GEEK, https://usabilitygeek.com/user-experience-and-security/ [https://perma.cc/8936-A3W2] (noting the need to balance user experience with security).

194. Steve Banker, *If Preventing a Cybersecurity Attack Is Impossible...*, FORBES (Mar. 3, 2015, 7:27 AM), https://www.forbes.com/sites/stevebanker/2015/03/03/if-preventing-cyber security-attacks-is-impossible/ [https://perma.cc/67YW-WAAX] ("[I]ntrusions may be all but certain for every organization."); ACCENTURE, THE NATURE OF EFFECTIVE DEFENSE: SHIFTING FROM CYBERSECURITY TO CYBER RESILIENCE 3 (2018), https://www.accenture.com/acnmedia/accenture/conversion-assets/dotcom/documents/local/en/accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf [https://perma.cc/3F2M-VUEC] ("Absolute security is absolutely impossible."); Daniel Dobrygowski, *Cyber Resilience: Everything You (Really) Need to Know*, WORLD ECON. F. (July 8, 2016), https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/ [https://perma.cc/8PHD-37DH] (comparing cybersecurity and cyber resilience).

195. *See* Toby Shackleton, *A Cost-Benefit Analysis Approach to Cyber Security*, SIX DEGREES (Mar. 3, 2021), https://www.6dg.co.uk/blog/cost-benefit-approach-to-cyber-security/ [https://perma.cc/7ZLU-4AGH].

196. *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1003-04 (2018) (explaining that, despite experiencing a cyber incident three years earlier, Sony continued to underinvest in cybersecurity measures—leading to a subsequent attack in 2014).

197. Gregory S. Gaglione, Jr., Comment, *The Equifax Data Breach: An Opportunity to*

face anything from financial damage, to humiliation, to longer-running harms.[198] Data insecurity makes individuals vulnerable not only to private actors but to governments as well. The U.S. government and others take full advantage of the porous information society ecosystem to learn about citizens for the purposes of public safety, crime prevention, and perhaps other, less wholesome purposes.[199]

Since the early 2000s, states have enacted data breach laws that provide public law enforcement with mechanisms intended to protect consumers' personal information.[200] Generally, such laws require companies maintaining consumer data to employ reasonable security practices and to notify consumers and state enforcement authorities when consumer data has been compromised.[201] However, they have failed to encourage companies to increase their standard of care at the pace at which hackers are improving their hacking techniques.[202]

In response to these concerns, some commentators have recently proposed support for public law regulations.[203] Some of these proposals advocate for new causes of action to be awarded due to the inadequacy of current tort and contract law to describe the nature of the threat represented by data insecurity.[204] Others argue that the main obstacle facing plaintiffs is the difficulty of proving harm and find that—rather than new causes of action—new ways of formalizing and recognizing the harm presented by data insecurity are needed.[205] There are also intermediate approaches. For example,

---

Improve Consumer Protection and Cybersecurity Efforts in America, 67 BUFF. L. REV. 1133, 1137-47 (2019) (describing the recent history of data breaches).

198. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 774 (2018).

199. Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 577 (2018) (describing the practice and outlining the law of government hacking).

200. *See* Carol M. Hayes, *Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Text*, 23 LEWIS & CLARK L. REV. 1221, 1223, 1249 (2020); Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193, 1235-36 (2020).

201. Hayes, *supra* note 200, at 1250-57.

202. Kosseff, *supra* note 196, at 1024-29 (describing the ways in which cybersecurity law is inadequate).

203. *See* Solow-Niederman, *supra* note 12, at 618.

204. *See id.*; Meglio, *supra* note 190, at 1241.

205. Solove & Citron, *supra* note 198, at 737-38.

Will McGeveran has suggested that existing law points toward a quasi-fiduciary duty of firms, which he calls "data custodians," to provide data security to individuals who have data in their charge.[206]

All of these proposals share an understanding that merely forcing companies to announce data breaches and subjecting them to public actions from state attorneys general is insufficient to prevent data insecurity. However, informational asymmetries create adverse incentive structures that lead to widespread data insecurity. Data breach notification laws rely on companies to report data breaches to consumers and state authorities.[207] Although these laws typically define "data breach," the company is left to make the initial determination as to whether a security incident requires public disclosure.[208] Such a regime presents the risk that companies may conceal borderline security events that come close, but not quite, to the level requiring disclosure. There is little incentive for firms to take initiative to invest in data security beyond public law standards. This is because most private actions against parties for data insecurity fail for lack of harm or lack of a case or controversy.[209] The reputational harm from data insecurity exists, but the evidence is mixed as to whether pure reputational harm influences the behavior of firms.[210]

Private enforcement fills this incentive lacuna by encouraging companies to protect consumer data even if it is possible to conceal their security failures from the regulator.[211] Imagine if failure to provide adequate data security could be considered a tort (or failure of some other legal obligation, perhaps in contract).[212] Because Software-as-a-Service (SaaS) has become the norm,[213] instead of selling or licensing software, most companies simply pay to use

206. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1139-40 (2019).

207. Hayes, *supra* note 200, at 1256.

208. *Id.* at 1252-55.

209. *See* Kosseff, *supra* note 196, at 1016.

210. *See id.* at 1016-17.

211. *See* Solow-Niederman, *supra* note 12, at 622 (discussing how a company's incentives change when framing privacy issues in a tort context).

212. *See id.* at 618.

213. *See* Samantha Schwartz, *2019 Trends: Cocktail of SaaS Applications Becomes the Norm*, CIO DIVE (Jan. 3, 2019), https://www.ciodive.com/news/2019-trends-cocktail-of-saas-applications-becomes-the-norm/544690/ [https://perma.cc/U97T-VQAU].

software owned and hosted by another firm.[214] In effect, SaaS concentrates responsibility for data security in a smaller number of firms. One of the advantages of SaaS is that data security liability can be contractually assigned to the SaaS provider.[215] Because the downstream firm (purchaser of SaaS) would face exposure to liability if the data security practices of the upstream firm were poor, the downstream firm would have the incentive to do due diligence and acquire appropriate insurance.[216] Having poor data security practices, then, would cost the SaaS provider business.[217] This would create an incentive to have strong data security practices outside of and parallel to data breach notification public law legislation. The private and public law avenues are mutually reinforcing, but note the essential nature of the private right of action.[218] A private right of action creates an incentive for private actors with more information and expertise about the relevant technology to hold each other accountable without the need to disclose their practices to the public.

Tort law imposes strict liability to discourage reckless behavior by forcing private actors to take every possible precaution.[219] Strict liability could be a powerful tool for preventing consumer exploitation from data leakage and data trafficking.[220] There is a great deal of precedent for this approach. The law imposes strict liability for dangerous items with long-ranging implications in other areas of the private law, including toxic torts[221] and products liability.[222] Databases pose predictable dangers to society, both when breached

---

214. Michael L. Rustad & Elif Kavusturan, *A Commercial Law for Software Contracting*, 76 WASH. & LEE L. REV. 775, 778-79 (2019).

215. W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 79, 92-94 (2012) (empirical study examining allocation of liability and risk in SaaS and other cloud contracts; found strong relationship between allocation of risk and bargaining power).

216. *See* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 193-94 (2017).

217. *See id.*

218. *See id.*

219. *See* Ormerod, *supra* note 12, at 1936.

220. *See id.* at 1936-38.

221. *See* McClain v. Metabolife Int'l, Inc., 401 F.3d 1233, 1237, 1240 (11th Cir. 2005); Adkisson v. Jacobs Eng'g Grp., Inc., 370 F. Supp. 3d 826, 835 (E.D. Tenn. 2019).

222. *See* Roverano v. John Crane, Inc., 226 A.3d 526, 528, 536 (Pa. 2020).

and when used as designed.[223] Danielle Citron has compared databases to reservoirs in the industrial age, arguing by analogy that data security breaches should trigger strict liability.[224] Peter Ormerod has gone further, suggesting that any information misuse violation also warrants strict liability.[225] That is not just the result of public legislation but also private law that keeps actors in society accountable to each other in order to preserve the dignity of the individual in all aspects of her life.[226] This shows the centrality of private law in regulating privacy. Without strict liability for data security harms, it is likely we will continue to see slipshod data practices.[227] Both the deterrence and dignitary justifications for private enforcement are present in motivating data security regulation. On the one hand, overall deterrence of data security practices is the aim of such regulation. But individuals can also face significant personal harms from data insecurity, and should not feel powerless to defend their personal information.

C. Data Power

Market power in the information age presents concerns that antitrust law is not competent to address without support from other forms of regulation.[228] A series of articles has attacked the status quo in the technology sector for promoting undue concentration of capabilities in the hands of a small group of companies.[229] Controlling a large database of granular consumer data accords the few owners of such databases powerful and unique abilities.[230] These capabilities are critical for the current day and even more important

223. Citron, *Reservoirs of Danger*, *supra* note 12, at 244-45, 291-93.

224. *See id.* at 291-93.

225. *See* Ormerod, *supra* note 12, at 1936-38.

226. *See id.*

227. *See id.* at 1944-46.

228. *See* Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES L. 189, 190, 194, 215 (2019); *cf.* Kristelia A. García, *Facilitating Competition by Remedial Regulation*, 31 BERKELEY TECH. L.J. 183, 246-47 (2016) (arguing for regulation that discourages industry cooperation and punishes lack of competition in the technology space).

229. *See, e.g.*, Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1053-54 (2017).

230. *See id.* at 1083-89.

for our future.[231] Artificial Intelligence (AI) and machine learning are important resources and only look to become more important with time.[232] The basic tools for machine learning and AI are taught to every computer science student at the college level.[233] But machine learning is only as strong as the size of its training set.[234] Without access to the databases that the Big Five technology companies control, there are limits to the quality of output even the best coded machines can produce.[235] Current methods of AI and machine learning development rely on large banks of data.[236] Therefore, the companies that have the most data will get the best results and be able to develop higher quality AI and machine learning applications and products.[237] So the possession of data creates dividends for entering new industries and will continue to dominate in the future, unless the basic method by which AI and machine learning changes.[238]

There are major economic implications of the combination of influence and outsized ability to innovate that big players in the information economy currently enjoy.[239] Orla Lynskey argues that, due to these specific characteristics, it is more useful to refer to data

---

231. *See id.* at 1083-89.

232. *See* C. Scott Hemphill, *Disruptive Incumbents: Platform Competition in an Age of Machine Learning*, 119 COLUM. L. REV. 1973, 1978-81 (2019).

233. *See generally* Justin Aglio, *An Inside Look—America's First Public School AI Program*, GETTING SMART (Jan. 4, 2019), https://www.gettingsmart.com/2019/01/04/an-inside-look-americas-first-public-school-ai-program/ [https://perma.cc/CRF9-G3C2] (describing the AI and machine learning program required for all Montour Public School District fifth through eighth grade students).

234. *See* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 677-81 (2017) (describing the need for sufficient data to train a machine learning system).

235. *See* Hemphill, *supra* note 232, at 1978-81 ("Machine learning advances also reinforce the importance of access to data. A larger stock of searches and observed outcomes—for example, whether the user clicked—generates data needed to train and improve the prediction of the algorithm. The importance of scale is heightened by the high variability of user data.... Considered as a whole, advances in machine learning tend to reinforce the market position of the leading platforms. There is reason to agree with the *Economist*'s assessment, emphasizing various advantages of the incumbents: 'It seems likely that the incumbent tech groups will capture many of AI's gains, given their wealth of data, computing power, smart algorithms and human talent, not to mention a head start on investing.'" (footnotes omitted)).

236. *See id.*

237. *See id.*

238. *See id.*

239. *See* Bamberger & Lobel, *supra* note 229, at 1083-87.

power in this context rather than the more generic term "market power."[240] I agree and will use the term throughout this Article.

Data power allows tech giants to act as gatekeepers in the information economy, empowering them to set norms for consumers and policies for downstream companies.[241] Even governments take advantage of the influence of companies with data power to achieve regulatory goals in the area of data protection.[242] Business models in the information economy are based on a "grow fast or die" model, in contrast to the industrial age model of incremental growth.[243] Modern startups aim to grow fast enough to attract the attention of one of the larger companies in order to be purchased.[244] Only in rare hypergrowth situations do even successful companies become worthy of continuing in their own right.[245] A startup company that looks to be able to profitably stand on its own even in the medium run is "a unicorn"—a whimsical way to convey its extreme unlikelihood.[246] Because few information-economy firms even hope or intend to continue in perpetuity, maintaining relationships with companies with more data power becomes critically important.[247] A startup's prospects of seriously competing against the most data-powerful companies are grim.[248] If one has a useful and popular application that would benefit from stronger AI, the current market incentivizes attempting to be acquired by Alphabet or Amazon rather than trying to build from scratch the type of information mine those

240. *See* Lynskey, *supra* note 228, at 190, 194, 215.

241. *See generally* Bamberger & Lobel, *supra* note 229, at 1086 ("There may be wide-ranging ways that Uber and other two-sided platforms can abuse their market power by taking advantage of the massive data they collect, to the detriment of both sides of the market.... By means of this information asymmetry, [Uber] can leverage 'access to information about users and their control over the user experience to mislead, coerce, or otherwise disadvantage sharing economy participants.'").

242. *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 469-72, 475-77 (2020).

243. *See* K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1626-27, 1650 (2018).

244. *See id.*

245. *See id.*

246. *See* Salvador Rodriguez, *The Real Reason Everyone Calls Billion-Dollar Startups 'Unicorns,'* INT'L BUS. TIMES (Sept. 3, 2015, 12:25 PM), https://www.ibtimes.com/real-reason-everyone-calls-billion-dollar-startups-unicorns-2079596 [https://perma.cc/VS6X-3F9K].

247. *See* BUS. ROUNDTABLE, *supra* note 5.

248. *See id.*

companies already have.[249] This type of incentive explains why the United States acknowledges many utilities as "natural" monopolies and regulates these monopolies accordingly.[250] It simply does not make any economic sense for multiple companies to run powerlines through the same community—it is more efficient to pool resources. Because of this similarity, some argue that a similar regime may be needed for companies with major data power.[251]

As the Cambridge Analytica scandal illustrates,[252] the rise of the platform economy means that the influence of data power goes beyond the mere exercise of power of the actor with data power.[253] If another company can leverage or siphon off the abilities of the monopolist, negative outcomes could arise outside the interests of the actor with market power itself.[254] The existence of data power, then, creates a certain type of threat because once it is there, it can be leveraged by anyone who gains access to it.[255] If antitrust law does not lead to the breakup of companies with data power—and even if it does—data power may have many of the characteristics of

---

249. *See* John Mannes, *Facebook, Amazon, Google, IBM, and Microsoft Come Together to Create the Partnership on AI*, TECHCRUNCH (Sept. 28, 2016, 5:01 PM), https://techcrunch.com/2016/09/28/facebook-amazon-google-ibm-and-microsoft-come-together-to-create-historic-partnership-on-ai/ [https://perma.cc/AS9N-2T9R].

250. *See id.*

251. *See, e.g.*, Rahman, *supra* note 243, at 1637 ("Industries triggered public utility regulation when there was a combination of economies of scale limiting ordinary accountability through market competition and a moral or social importance that made the industries too vital to be left to the whims of the market or the control of a handful of private actors. This combination of economic dominance and social necessity is what created the threat of not just exploitative prices but also discrimination and unequal access."); Adam Candeub, *The Common Carrier Privacy Model*, 51 U.C. DAVIS L. REV. 805, 809, 846-47 (2018) (arguing for imposing common carrier liability on internet companies to protect privacy).

252. *See, e.g.*, Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/7LY7-EYX5] (detailing how Cambridge Analytica built an algorithm to determine voting behavior by harvesting data from more than fifty million Facebook profiles through an online personality test that collected information on test-takers' Facebook friends).

253. *See* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 89-90 (2016).

254. *See generally* Cadwalladr & Graham-Harrison, *supra* note 252 (describing how Cambridge Analytica exploited access to Facebook profiles and networks and used the collected data for political and financial gain).

255. *See, e.g.*, *id.* ("[Cambridge Analytica] exploited Facebook to harvest millions of people's profiles. And built models to exploit what [Cambridge Analytica] knew about them and target their inner demons. That was the basis the entire company was built on.").

public utilities and should be regulated more like utilities and utility-like industries.[256] That is, legislators should not hesitate to provide specific rules that companies with data power must apply in order to serve the public interest, much like they do with banks, utilities, and other industries with major concentration that citizens must use to survive.

Data power, like other forms of market power, is a strange beast because it is not inherently bad to have just one provider of a given service, or just one actor in control of a resource.[257] Problems arise because the monopolist, given that no other actor is in a position to stop her, can take advantage of her position by offering higher prices or lower-quality goods.[258] Also, absent the threat of competition, a monopolist lacks the incentive to innovate and provide better services.[259] Instead, the monopolist is more inclined to expend resources suppressing and acquiring competition.[260] After the Gilded Age highlighted the dangers of an economy dominated by companies with market power, Congress enacted antitrust laws to protect consumers from exploitation and to provide would-be competitors an opportunity to compete.[261]

Several authors pointedly compare the rise of technology companies with data power over the past two decades to the Gilded Age, dubbing it the New Gilded Age.[262] And indeed, one can observe both negative characteristics described above in the current operating of major information-economy firms.[263] Consider the data protection

256. *See* Rahman, *supra* note 243, at 1650.

257. Barak Orbach, *How Antitrust Lost Its Goal*, 81 FORDHAM L. REV. 2253, 2263-64 (2013).

258. *Id.* at 2265.

259. *See id.* at 2271.

260. *See id.* at 2262.

261. *See* TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 45-58 (2018); *see also* Orbach, *supra* note 257, at 2262 ("The members of Congress undoubtedly intended to address the 'trust problem,' but their lack of direct discussion of the merits of competition is puzzling.").

262. *See generally* Tom Wheeler, *Who Makes the Rules in the New Gilded Age?: Lessons from the Industrial Age Inform the Information Age*, BROOKINGS (Dec. 12, 2018), https://www.brookings.edu/research/who-makes-the-rules-in-the-new-gilded-age/ [https://perma.cc/GH2V-VHZD] ("Today we live in the new Gilded Age: technology-driven innovations have again improved daily life while creating great wealth, inequality of circumstances, non-competitive markets, and viral deceit.").

263. *Compare* Maurice E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, HARV. BUS. REV. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-

policy of the Big Five's email and messaging services.[264] There is no option to refuse to have your data processed or shared with partner companies.[265] While some argue that consumers love getting free services and accept the "cost" of invasive data practices,[266] that argument presumes a free market.[267] If we presume market power, there is another, market-power-oriented reason for the availability of information services that do not provide much data protection.[268] When the price stays the same (free), offering a lower-quality product is the equivalent of charging a higher price than the free market would offer.[269] It is the ability of the actor with market power to demand more of the public than a free market would permit.[270] Secondly, we also see the Big Five working to buy their competition.[271] Absorption is one way of holding true competition and innovation in check. What is more, some observers note that the rate of actual change in experience presented by technology has slowed over the past ten to fifteen years relative to the 1990s and early 2000s.[272] This coincides with the rise of a set of firms with serious data power.[273]

---

data [https://perma.cc/GAH9-KJQY], *with supra* notes 256-60 and accompanying text.

264. *See* Alex Hern, *Privacy Policies of Tech Giants 'Still Not GDPR-Compliant*,*'* THE GUARDIAN (July 4, 2018, 7:01 PM), https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant [https://perma.cc/ND59-RSPX].

265. *See id.*

266. *Cf., e.g.*, Ellis Hamburger, *Consumers Pay the Hidden Costs for the 'Free' App Ecosystem*, THE VERGE (Jan. 7, 2013, 9:31 AM), https://www.theverge.com/2013/1/7/3835724/the-price-of-apps [https://perma.cc/H5C7-Q3FP].

267. Nicholas Economides & Ioannis Lianos, *Giving Away Our Data for Free Is a Market Failure*, PROMARKET (Feb. 1, 2021), https://promarket.org/2021/02/01/free-data-market-failure-digital-platforms/ [https://perma.cc/63GL-WZAB].

268. *See id.*

269. *See* Hamburger, *supra* note 266.

270. *See* Economides & Lianos, *supra* note 267 ("[W]e observe a *market failure* where all transactions occur at the same zero price, and some transactions that would have occurred under competition do not occur. The market failure is a direct result of the imposition of the take-it-or-leave-it contract by dominant digital platforms and the default opt-in.").

271. *See* Gerrit De Vynck & Cat Zakrzewski, *Tech Giants Quietly Buy up Dozens of Companies a Year. Regulators Are Finally Noticing.*, WASH. POST (Sept. 22, 2021, 7:59 PM), https://www.washingtonpost.com/technology/2021/09/20/secret-tech-acquisitions-ftc/ [https://perma.cc/68Z4-DWX6].

272. *See id.*

273. *See generally* Economides & Lianos, *supra* note 267 (crediting mergers between smaller companies and large "voracious[ ] collect[ors of] personal information" like Google and Facebook and the resulting market dominance of the Big Five as a primary driver of "[t]he ability of the digital platforms to drive users to accept their take-it-or-leave-it opt-in contract

Antitrust law is a hybrid enforcement regime, including a private right of action for parties impacted by unfair competition, providing for treble damages for successful cases in order to enhance deterrence.[274] The Supreme Court has specifically noted the significance of deterrence in the reason for this measurement of relief.[275] A 2008 empirical study of forty cases showed that private enforcement was a key source of deterrence for anticompetitive behavior, noting: "almost half of the underlying violations were first uncovered by private attorneys, not government enforcers, and that litigation in many other cases had a mixed public/private origin."[276] The authors concluded that private enforcement likely does more to deter anticompetitive conduct than public enforcement.

As of the early 2000s, the Supreme Court has sought to limit private enforcement in antitrust law.[277] Notably, in 2004, in *Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko*, the Court worried about the cost of false positives in antitrust litigation, and the dangers of potential "chilling effects" to industry.[278] The increasing concentration of the technology industry counsels reconsideration of this skepticism of private enforcement in antitrust. Privacy is among the key dignitary concerns that commentators flag

---

to provide personal data at zero price").

274. 54 AM. JUR. 2D *Monopolies and Restraints of Trade* § 305 (2022) ("Congress has encouraged private antitrust litigation not merely to compensate those who have been directly injured, but also to vindicate the important public interest in free competition. The Clayton Act functions as the private enforcement mechanism for claims brought under the federal antitrust laws. The Act generally allows private persons to sue for treble damages or injunctive relief. Such injunctive relief may include divestiture. The availability of a private antitrust action, and its accompanying treble-damages remedy, serves both to compensate private persons for their injuries and to punish wrongdoers. Private enforcement of the nation's antitrust laws also increases the likelihood that violators will be discovered." (footnotes omitted)).

275. *See, e.g.*, Zenith Radio Corp. v. Hazeltine Rsch., Inc., 395 U.S. 100, 130-31 (1969) ("[T]he purpose of giving private parties treble-damage and injunctive remedies was not merely to provide private relief, but was to serve as well the high purpose of enforcing the antitrust laws."); Minn. Mining & Mfg. Co. v. N.J. Wood Finishing Co., 381 U.S. 311, 318 (1965) ("Congress has expressed its belief that private antitrust litigation is one of the surest weapons for effective enforcement of the antitrust laws.").

276. Robert H. Lande & Joshua P. Davis, *Benefits from Private Antitrust Enforcement: An Analysis of Forty Cases*, 42 U. S.F. L. REV. 879, 880 (2008).

277. Edward D. Cavanagh, *The Private Antitrust Remedy: Lessons from the American Experience*, 41 LOY. U. CHI. L.J. 629, 636 (2010).

278. 540 U.S. 398, 414 (2004).

when concerns are raised about data power.[279] While deterrence is traditionally preeminent in rationales for private antitrust enforcement, compensation and retribution for other firms effected are a powerful alternate rationale for private enforcement of antitrust.[280] Nicholas Cornell has recently articulated a justification for private enforcement of antitrust as a "form of accountability between parties," showing how public regulatory law can give rise to "private moral grievances."[281]

D. Digital Market Manipulation

Digital market manipulation is using personal information to unilaterally determine citizens' preferences and behaviors.[282] Ryan Calo showed that digital market manipulation substantively differs from pre-information age forms of persuasion in three ways: (1) "'the mass production of bias' through big data," (2) "the possibility of far greater consumer intelligence through 'disclosure ratcheting,'" and (3) "the move from ends-based to means-based ad targeting and interface design."[283] Advanced methods called "dark patterns" intensify the ability of applications designed to manipulate consumers.[284] "Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions."[285] Brett Frischmann

279. *See* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right *[Approach]* to Privacy, 80 ANTITRUST L.J. 121, 132 (2015); Stucke, *supra* note 263.

280. *See generally* Sanjukta Paul, *Recovering the Moral Economy Foundations of the Sherman Act*, 131 YALE L.J. 175, 179 (2021).

281. Nicolas Cornell, *Competition Wrongs*, 129 YALE L.J. 2030, 2037 (2020).

282. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1000 (2014); Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449 (2019).

283. Calo, *supra* note 282, at 1006-07.

284. *See* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 43-44 (2021) ("[The article] discusses the results of the authors' two large-scale experiments in which representative samples of American consumers were exposed to dark patterns.... [Based on their findings, the authors concluded] [m]any dark patterns appear to violate federal and state laws restricting the use of unfair and deceptive practices in trade.").

285. Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM ON HUM.-COMPUT. INTERACTION, Nov. 2019, at 81:1, https://arxiv.org/pdf/1907.07032.pdf [https://perma.cc/6CW7-8FEU].

and Evan Selinger describe the extensive intervention in consumer behavior as inducing humans to behave like "simple machines," without the people so shaped even realizing it.[286] The most famous instance of this is the Cambridge Analytica scandal of 2017.[287] The ability of private elites to influence citizen opinions is not new and may be inevitable to some degree.[288] Yet there are concerns that the granular degree of control companies have over what individuals see and experience could enable an unprecedented degree of effective mind control with the potential to undermine democracy.[289]

Private enforcement enables individuals to wield the law when they determine that their legal rights have been violated.[290] Public enforcement is removed from the lived relationship between parties in society.[291] The adversarial nature of the American justice system allows for the ongoing analysis and evolution of the nature and character of violation of the rights and responsibilities members of society have against one another.[292]

These procedural inputs are of fundamental importance in the case of digital market manipulation. Unlike, for example, salesmanship versus fraud, there is not a common cultural baseline that

---

286. BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 6 (2018).

287. *See* Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH. L. & POL'Y 43, 97, 99, 125 (2020); *see also supra* notes 251-54.

288. JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM & DEMOCRACY 263 (1944) ("The only point that matters here is that, Human Nature in Politics being what it is, [leaders] are able to fashion and, within very wide limits, even to create the will of the people. What we are confronted with in the analysis of political processes is largely not a genuine but a manufactured will. And often this artefact is all that in reality corresponds to the *volonté générale* of the classical doctrine. So far as this is so, the will of the people is the product and not the motive power of the political process."); Joseph A. Schumpeter, *Excerpt from Capitalism, Socialism and Democracy* (1942), *in* THE IDEA OF THE PUBLIC SPHERE: A READER 54 (Jostein Gripsrud et al. eds., 2010) ("Schumpeter's interest in mass society and crowd psychology ... led him to underline influence of advertising and other methods of persuasion. He regarded it as evident that 'the will of the people' could be fabricated or manufactured by the rulers and that a genuine public participation in politics therefore was an illusion. The public sphere in Schumpeter's approach is reduced to a market and a competitive arena for elite groups.").

289. *See* FRISCHMANN & SELINGER, *supra* note 286, at 6.

290. LAHAV, *supra* note 107, at 32, 39.

291. *See id.* at 39 ("American society values decentralization and individualized enforcement of the law as opposed to enforcement through a bureaucracy engaged in centralized decision-making. Private litigation reflects these values.").

292. *See id.* at 32, 39.

allows individuals to intuitively understand the difference between digital market manipulation and puffery.[293]

The limit of public enforcement in the case of techno-social engineering comes from several characteristics of the administrative state. The extent to which government can understand social norms without the facts and context presented in cases between individuals is limited.[294] As many technological applications are developed outside of government, private individuals and firms will often have a superior understanding of the first-level functionings of the technology and the second-order social workings of that technology.[295] An example of these two levels can be found in the workings of the popular social media platform Twitter. Twitter has a variety of complicated coding and moderation characteristics mostly unavailable to the public; these characteristics represent the first-level technical functionings that may be difficult for government actors to understand.[296] Customers' practical use of the application comprises the second-order social level. The Twitter search function using "hash" emerged organically among users, not from the central programming of the app.[297]

As long as the boundaries of digital market manipulation are in flux, companies that control platforms can, to the extent possible, shield themselves from direct regulation and government scrutiny.[298] Such companies have an incentive to prevent the development of disadvantageous rules. While some writers have shown optimism about the command and control structure in digital

---

293. *Cf.* Raymond Shih Ray Ku, *Grokking* Grokster, 2005 WIS. L. REV. 1217, 1217 (defining the term "grok" as a synonym for understanding intuitively, discussing its use in a techlaw context).

294. *See* Kerry, *supra* note 142.

295. *See* Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 370, 386-87 (2016).

296. *See* Mulligan & Bamberger, *supra* note 113, at 701-02; Joyce E. Cutler, *Lawmakers' Lack of Technical Expertise Worries ABA Science, Technology Leaders*, BLOOMBERG L. (Mar. 15, 2012), https://news.bloomberglaw.com/e-discovery-and-legal-tech/lawmakers-lack-of-technical-expertise-worries-aba-science-technology-leaders [https://perma.cc/RB5U-GSJS].

297. Lexi Pandell, *An Oral History of the #Hashtag*, WIRED (May 19, 2017, 7:00 AM), https://www.wired.com/2017/05/oral-history-hashtag/ [https://perma.cc/S8EK-TNYS] (describing the hashtag as starting from "early adopters ... developing tools to organize their tweets").

298. *See* Rory Van Loo, *The Corporation as Courthouse*, 33 YALE J. ON REGUL. 547, 554-55 (2016).

regulation,[299] effective digital regulation requires a real-world understanding of social-technical practices. Although adversarial litigation and arbitration do not perfectly simulate the features of new norms and technologies, public regulation relies substantially on material produced by interest groups, which is hardly more objective.[300] Government does not have a seat at the table in day-to-day development of technology and social practices, and the organic disputes that arise therefrom.[301] Thus, without the support of private enforcement, the government's direct understanding of and stake in such disputes is limited.[302]

Digital market manipulation puts the average citizen at the mercy of internet commerce companies, and subjects the citizen to arbitrary power by the platform owner.[303] Private enforcement would give the citizen some right of private action against the company for interfering with her self-determination and exposing her privacy invasions and data insecurity. This right could take the form of increased tort liability that cannot be disclaimed, implied contractual obligations that cannot be disclaimed, or some form of fiduciary duty owed by the company to the consumer.

Digital market manipulation could lead to major economic losses to individuals. According private rights of action to pursue them would provide an additional incentive to companies to avoid manipulative conduct, even when state regulatory bodies are overwhelmed or inactive. Furthermore, when a citizen feels wronged by a company's manipulative practice, according them the right to pursue their own claims, even if public regulatory bodies are disinterested in doing so, accords dignity to the citizen while pragmatically giving her the opportunity to seek relief when she has been wronged. Overall, discouraging manipulation in markets encourages markets based on actual consumer preferences rather than smoke and mirrors, which is better for society overall, as well as the progress of innovation.

299. *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1274 (2017).
300. *See, e.g.*, Van Loo, *supra* note 298, at 551-52.
301. *See* Cutler, *supra* note 296.
302. *See, e.g.*, Van Loo, *supra* note 298, at 592-93.
303. *See id.* at 550-51.

E. Government Surveillance

Government surveillance refers to the increased ability of government to surveil citizens.[304] The classic rule of law formulation states that citizens have a right to be free of arbitrary exercise of power.[305] Yet, the government's increasing access to personal information could effectively enable government to influence and control citizens.[306] Even commentators less worried about private-sector manipulation have expressed concerns about government wielding unchecked access to personal information about every citizen.[307] For example, following a deadly terrorist attack in 2015, the Department of Justice sought access to a suspect's encrypted iPhone.[308] Apple, a public company with direct relationships with consumers, bristled at the reputational harm from publicly turning over customers' information to the government.[309] Cases such as this highlight the intertwined relationship between private corporations and the government. As long as private actors have information or relationships that could be useful to the government, the government will pressure those private actors to share that information.[310] Even powerful companies such as Apple have an incentive to cooperate with government investigations and informal agency oversight to avoid backlash in the form of unfavorable legislative or policy decisions.[311] Ultimately, no private actor can match the

304. *See* Jonathan Vanian, *How Digital Surveillance Thrived in the 20 Years Since 9/11*, FORTUNE (Sept. 8, 2021, 5:15 AM), https://fortune.com/2021/09/08/digital-privacy-patriot-act-9-11/ [https://perma.cc/P3XF-UUB4].

305. *Cf.* Robert A. Stein, *What Exactly Is the Rule of Law?*, 57 HOUS. L. REV. 185, 187-89 (2019).

306. *See* Stucke, *supra* note 263.

307. *E.g.*, Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 1003 (1999).

308. Julia P. Eckart, *The Department of Justice Versus Apple Inc.—the Great Encryption Debate Between Privacy and National Security*, 27 CATH. U. J.L. & TECH. 1, 4-6 (2019) (describing the history and implications of the dispute between Apple and the DOJ following the San Bernadino shooting).

309. *Id.* at 41.

310. *See* Stucke, *supra* note 263.

311. *See* Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319, 333 (2002) ("Political choice theory teaches that regulatory schemes are influenced by political actors and interest groups, making it difficult to predict the underlying goals ex ante. Even if there are clear normative goals at the outset, the political process may lead to other goals. Some regulatory

government's power; this asymmetry is by design. The fundamental purpose of government involves bringing all nongovernment actors under the state's control—at least to some degree.[312]

Though the Fourth Amendment limits the government's ability to perform searches and seizures, in many cases, the third party disclosure rule allows the government to access indirectly what it cannot directly.[313] Even assuming arguendo that reputation serves as a check against private-sector privacy abuses, such a check does not apply to the federal government's potential privacy violations. This is because, as the Snowden disclosures revealed, many of the court determinations permitting federal access to personal information data are—by design—not public.[314] However, many of the most significant data traffickers with broad-based information about every American are not even public-facing entities in direct contract with consumers, so they also do not face reputational concerns.[315] A handful of magistrate judges, keenly worried about the potential impropriety of the government accessing too much information, have erected somewhat higher standards for government access to privately held information.[316]

When it comes to privacy and data security threats, private and public actors are a two-headed monster. One inevitably feeds the

---

schemes thus will favor efficiency goals, some may favor distributional and other non-efficiency goals, and some may combine these goals. One cannot always assume that efficiency is the sole goal of commercial regulation." (footnotes omitted)).

312. *See* Joseph S. Nye, Jr., *Public Diplomacy and Soft Power*, 616 ANNALS AM. ACAD. POL. & SOC. SCI., 94, 101-02 (2008); E.A. Goerner & Walter J. Thompson, *Politics and Coercion*, 24 POL. THEORY 620, 621 (1996); *see also* THOMAS HOBBES, LEVIATHAN 106 (J.C.A. Gaskin ed., Oxford World Classics 1996) ("These dictates of reason, men used to call by the name of laws; but improperly: for they are but conclusions, or theorems concerning what conduceth to the conservation and defence of themselves; whereas law, properly is the word of him, that by right hath command over others."). *But see* Eichensehr, *supra* note 12, at 669 (considering the idea of powerful technology companies as politically neutral peers of traditional governments).

313. *See* Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1444 (2017).

314. Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679, 1683-85 (2015); *see also* Jonathan Manes, *Secret Law*, 106 GEO. L.J. 803, 806 (2018).

315. *See* Scholz, *supra* note 84, at 663-64.

316. *See generally* Emily Berman, *Digital Searches, the Fourth Amendment, and the "Magistrates' Revolt*," 68 EMORY L.J. 49, 53 (2018) (describing the "outsized effect" of judicial limitations placed on government access of personal information during the so-called Magistrates' Revolt, including requiring the government to disclose the intended duration of the data seizure and its plan for any information that may be recovered outside of the intended basis for the application, to obtain a warrant).

other, and both are inextricably linked, because under the third-party doctrine, government agencies can usually demand access to most information a company has.[317] Modern practices have it that third parties collectively hold most information about the average person. So in order to truly eradicate a certain type of privacy risk to citizens, a comprehensive approach—incorporating both public and private enforcement—is required. The laws governing private actors' informational transactions necessarily shape and limit the government's reach, because the government can obtain data from private parties that it could not legally access directly.[318] Much of this transfer can even happen outside of the formal channels of warrant acquisition.[319] The only real way to prevent the government from acquiring a certain type of information is to limit private actors' ability to acquire such information, or to put certain limitations on their acquisition, such as data minimization policy.

The possibility that public actors may access private actors' data stockpiles is one of several reasons why private parties should not possess powers that threaten the rule of law.[320] If our goal is to prevent the state from accessing certain data sources, private enforcement must inhibit the compilation of such data.[321] Otherwise, public law alone cannot prevent the state from exercising the same powers that animate rule of law concerns when the government acts or acquires directly.[322] Private enforcement claims that discourage "collect-it-all" databases would also limit the government's ability to be parasitic on those databases.[323] Examples of potential private rights of action include a negligence action against a provider whose policies insufficiently protected user data, or a breach of the implied duty of good faith if appropriate representations about data security were made between two contracting parties.[324] Several

317. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018); Smith v. Maryland, 442 U.S. 735 (1979). The third-party doctrine has been criticized as a state intrusion on individual privacy. *E.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

318. Richards, *supra* note 313, at 1444.

319. *Id.*

320. *See supra* notes 240-41 and accompanying text.

321. *See, e.g.*, Kerry, *supra* note 142.

322. *See* Stein, *supra* note 305, at 187-89; Stucke, *supra* note 263.

323. *See, e.g.*, Kerry, *supra* note 142.

324. *See, e.g.*, Solow-Niederman, *supra* note 12, at 619-22.

commentators have suggested novel tort private rights of actions against actors with poor data security practices.[325]

Limiting private actors' ability to exert arbitrary power directly on consumers also prevents the government's ability to exert arbitrary power indirectly through private actors.[326] Limiting a private company's ability to exert arbitrary power not only prevents that company from exploiting consumers directly but also prevents the government from exploiting consumers through companies.

CONCLUSION

Private rights of action have a critical role to play in privacy regulation. If legislators and stakeholders want privacy laws to make a difference, private enforcement of privacy rights is imperative. Privacy laws will lack effectiveness without private litigants adding accountability through public pressure and additional enforcement. Private rights of action are a fixture in regulating many complex and pervasive areas of life and commerce, and indeed have been included in several of the most effective federal privacy laws. The importance, complexity, and prevalence of privacy issues in society makes hybrid enforcement necessary for resilient privacy regulation.

In addition to increasing the effectiveness of the law, private rights of action make the content of the law more responsive to social and technological realities by allowing judicial decisions to develop nuance in the application of legislation. Pleadings, motion practice, and discovery allow the deliberative, public processing of information about privacy practices and encourages a public conversation about and processing of privacy norms.

Finally, private enforcement honors the common law roots of privacy in the United States. In their influential article that was the first to describe the right to privacy in American law, Louis Brandeis and Samuel Warren characterized privacy as a dignitary right possessed by each person in their personality, which flowed directly from our common law tradition.[327] It would be wrong to

325. Ormerod, *supra* note 12, at 1896, 1919; Ludington, *supra* note 12, at 146.

326. *See* Stucke, *supra* note 263.

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

deny an individual the power to enforce such a bedrock right simply because a public agency declined to enforce it. The concept of privacy, taken seriously, should allow individuals the opportunity to contest privacy wrongs through legal process. The question of whether to make a claim based on a dignitary right in one's personality should not come down to an agency's decision. According individuals the power to vindicate their privacy rights would be an important step towards creating an information society that recognizes and values citizens.

Concerns about private enforcement leading to too much deterrence should be addressed in light of these two independent justifications for private enforcement. Such concerns may lead lawmakers to offer limited private enforcement or limit relief. But the drastic act of providing no private enforcement avenue at all for new privacy laws has the potential to doom their success from the start.