Notre Dame Law Review

Volume 98 | Issue 1 Article 5

11-2022

Privacy Qui Tam

Peter Ormerod
Assistant Professor of Law, Northern Illinois University College of Law

Follow this and additional works at: https://scholarship.law.nd.edu/ndlr

 Part of the Legal Remedies Commons, and the Privacy Law Commons

Recommended Citation

Peter Ormerod, *Privacy Qui Tam*, 98 Notre Dame L. Rev. 267 (2022).
Available at: https://scholarship.law.nd.edu/ndlr/vol98/iss1/5

This Article is brought to you for free and open access by the Notre Dame Law Review at NDLScholarship. It has been accepted for inclusion in Notre Dame Law Review by an authorized editor of NDLScholarship. For more information, please contact lawdr@nd.edu.

PRIVACY QUI TAM

*Peter Ormerod**

Privacy law keeps getting stronger, but surveillance-based businesses have proven immune to these new legal regimes. The disconnect between privacy law in theory and in practice is a multifaceted problem, and one critical component is enforcement.

Today, most privacy laws are enforced by governmental regulators—the Federal Trade Commission, the nascent California Privacy Protection Agency, and state attorneys general. An enduring impasse for proposed privacy laws is whether to supplement public enforcement by using a private right of action to authorize individuals to enforce the law.

Both of these conventional enforcement schemes have significant shortcomings. Public enforcement has proven inadequate because resource-constrained regulators only rarely bring enforcement actions, and the resulting consent decrees tend to entrench the status quo. Meanwhile, private enforcement is increasingly infeasible thanks to defendant-friendly Supreme Court decisions about the Federal Arbitration Act, Article III standing, and class action certification.

This Article proposes a hybrid approach: policymakers should enact privacy laws that authorize qui tam enforcement. A qui tam is an ancient legal action that authorizes a private plaintiff called a relator to redress an injury suffered by society, and successful relators are entitled to a portion of the recovery. A privacy qui tam is responsive to the shortcomings with both public and private enforcement: individuals are empowered to sue lawbreakers, but these suits don't face the same obstacles as private rights of action.

Qui tam has traditionally protected collective rights, so a crucial question about the viability of a privacy qui tam is whether violations of privacy law could be considered collective injuries amendable to qui tam enforcement. Fortunately, privacy scholars in recent years have convincingly shown that privacy is a social phenomenon that requires policy intervention at a structural level. A privacy qui tam therefore operationalizes privacy theory and promises to fill the enforcement void left by overwhelmed regulators and infeasible private rights of action.

© 2022 Peter Ormerod. Individuals and nonprofit institutions may reproduce and distribute copies of this Article in any format at or below cost, for educational purposes, so long as each copy identifies the author, provides a citation to the *Notre Dame Law Review*, and includes this provision in the copyright notice.

* Assistant Professor of Law, Northern Illinois University College of Law. For their valuable comments on earlier drafts of this Article, I'm grateful to Patricia Sánchez Abril, Roger Ford, Sarah Fox, Ivy Gibson, Robert Jones, and Jeffrey Omari. Thanks also to Spencer Faircloth for essential research assistance.

INTRODUCTION

The conventional wisdom is that privacy law is undergoing a revolution. In 2018, the European Union implemented the General Data Protection Regulation (GDPR) and California enacted the California

Consumer Privacy Act (CCPA),[1] and these legal regimes impose a host of novel duties on companies that profit from users' information.[2] Others soon followed: Virginia, Colorado, and Utah enacted omnibus privacy laws,[3] and California later supplemented its earlier law through a ballot measure.[4] Nevada, Vermont, and Maine enacted more targeted proposals.[5] Nearly a dozen comprehensive privacy bills have been proposed in Congress, while most statehouses are debating similar measures.[6]

But this revolution is only a façade. Informational businesses have proved remarkably unaffected by these new privacy laws. Digital advertising revenue soared to a record $189 billion in 2021, a 35% annual increase and up 591% since 2011.[7] Surveillance-based businesses have frequently reported record-shattering earnings and profits.[8] An average person encounters as many as ten thousand advertisements every day, many of which are the byproduct of pervasive surveillance both online and off.[9] Companies nevertheless seek ever more exotic ways

1 *See generally* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]; California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022).

2 *See infra* Section I.A.

3 *See generally* VA. CODE ANN. §§ 59.1-575–59.1-585 (2022); COLO. REV. STAT. §§ 6-1-1301 to 6-1-1313 (2022); UTAH CODE ANN. §§ 13-2-1 to 13-2-9 (West 2022).

4 *See* California Privacy Rights Act of 2020, Proposition 24 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–1798.199.100).

5 *See* NEV. REV. STAT. § 603A.345 (2021) (empowering users to opt out of having their data sold to third parties); VT. STAT. ANN. tit. 9, §§ 2446–47 (2022) (tightening regulation of data brokers); ME. STAT. tit. 35-A, § 9301 (2022) (restricting internet service providers' ability to disclose customer data).

6 *See* Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 21 nn.2–3 (2021).

7 *See Digital Advertising Soared 35% to $189 Billion in 2021 According to the IAB Internet Advertising Revenue Report*, INTERACTIVE ADVERT. BUREAU (Apr. 12, 2022), https://www.iab.com/news/digital-advertising-soared-35-to-189-billion-in-2021-according-to-the-iab-internet-advertising-revenue-report/ [https://perma.cc/K6FD-MF99]; *Digital and Non-digital Advertising Revenue*, PEW RSCH. CTR. (July 27, 2021), https://www.pewresearch.org/journalism/chart/sotnm-digital-and-non-digital-advertising-revenue/ [https://perma.cc/YK8Y-EQPP].

8 *See, e.g.*, Daisuke Wakabayashi, *Alphabet's Profit Increased 36 Percent, to $20.64 Billion, in the Fourth Quarter.*, N.Y. TIMES (Feb. 1, 2022), https://nytimes.com/2022/02/01/technology/google-alphabet-earnings.html [https://perma.cc/T73Q-HMZT]; Jonathan Ponciano, *Facebook Posts Record $29 Billion in Second-Quarter Revenue—Blowing Past Wall Street Expectations*, FORBES (July 28, 2021, 4:22 PM), https://forbes.com/sites/jonathanponciano/2021/07/28/facebook-earnings/ [https://perma.cc/LXZ2-4UUA].

9 *See* Sam Carr, *How Many Ads Do We See a Day in 2022?*, LUNIO (Feb. 15, 2021), https://ppcprotect.com/blog/strategy/how-many-ads-do-we-see-a-day/ [https://perma.cc/P6BB-LNTB] (advertising estimate); Zoe Schiffer, *Facebook and Google Surveillance Is an 'Assault on*

to surveil us, and they demand ever more places to insert algorithmically determined and user-specific commercial messages—despite high-profile mishaps.[10] Prominent enforcement actions are bottlenecked inside a small number of industry-captured regulators, and even successful actions have extracted disappointing penalties and underwhelming concessions.[11] Privacy scholars have condemned even the newest and strongest regulations as insipid, porous, and ineffective.[12] To the extent that new privacy rules have affected informational businesses' bottom lines, privacy *law* has had next to nothing to do with it. Instead, corporate-imposed mandates have had a limited effect on profit-driven surveillance,[13] and companies are successfully finding ways to circumvent even these modest restrictions.[14]

Privacy,' Says Amnesty International, THE VERGE (Nov. 20, 2019, 7:13 PM), https://theverge.com/2019/11/20/20974832/facebook-google-surveillance-data-assault-privacy-amnesty-international [https://perma.cc/D5TW-SDQ6] (online surveillance); Julia Angwin, Surya Mattu & Terry Parris Jr., *Facebook Doesn't Tell Users Everything It Really Knows About Them*, PROPUBLICA (Dec. 27, 2016, 9:00 AM), https://propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them [https://perma.cc/CHT4-6BRD] (offline surveillance).

10 *See, e.g.*, Steven Zeitchik, *Former Google Scientist Says the Computers That Run Our Lives Exploit Us—and He Has a Way to Stop Them*, WASH. POST (Jan. 17, 2022, 6:00 AM), https://washingtonpost.com/technology/2022/01/17/artificial-intelligence-ai-empathy-emotions/ [https://perma.cc/MN9K-A4WC] (using machine learning to analyze people's emotions); Ashley Carman, *Podcasters Are Letting Software Pick Their Ads—It's Already Going Awry*, THE VERGE (Jan. 4, 2022, 8:30 AM), https://theverge.com/2022/1/4/22865034/podcast-programmatic-spotify-ad-network [https://perma.cc/4567-YGSZ] (inserting programmatic advertising into podcasts).

11 *See* Nicholas Vinocur, *'We Have a Huge Problem': European Tech Regulator Despairs over Lack of Enforcement*, POLITICO (Dec. 27, 2019, 5:04 AM), https://politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605 [https://perma.cc/M77Q-F7C4]; *see also infra* notes 153–56, 166–69 and accompanying text.

12 *See, e.g.*, JULIE E. COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, 3–8 (2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/DY8J] (criticizing current approaches); Waldman, *supra* note 6, at 40–41 (surveying scholars' alternatives); *see also infra* Section I.B.

13 *See, e.g.*, Kate Conger & Brian X. Chen, *A Change by Apple Is Tormenting Internet Companies, Especially Meta*, N.Y. TIMES (Feb. 3, 2022), https://nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.html [https://perma.cc/G9CP-J5A4]; Emma Roth, *Apple's App Tracking Policy Reportedly Cost Social Media Platforms Nearly $10 Billion*, THE VERGE (Oct. 31, 2021, 6:13 PM), https://theverge.com/2021/10/31/22756135/apple-app-tracking-transparency-policy-snapchat-facebook-twitter-youtube-lose-10-billion [https://perma.cc/L5HE-37FA].

14 *See* Patrick McGee, *Apple Reaches Quiet Truce over iPhone Privacy Changes*, FIN. TIMES (Dec. 8, 2021), https://www.ft.com/content/69396795-f6e1-4624-95d8-121e4e5d7839 [https://perma.cc/LNF9-YY5S]; Patrick McGee, *Apple Under Pressure to Close Loopholes in New Privacy Rules*, FIN. TIMES (June 7, 2021), https://www.ft.com/content/9cb52394-f95f-4b07-a624-89c47439aa16 [https://perma.cc/D2S3-T6GV].

Privacy scholars are increasingly investigating why privacy law is proving so toothless.[15] The tenuous relationship between privacy law in theory and privacy law in practice is a multifaceted problem, and one crucial component of this phenomenon concerns enforcement.[16]

Most privacy laws are publicly enforceable: a governmental entity is charged with pursuing lawbreakers. For example, the European Union's and California's new privacy laws are both publicly enforceable, and the Federal Trade Commission (FTC) is the preeminent federal regulator of information privacy in the United States.[17] On the other hand, some privacy laws empower individuals to enforce them. For example, the Fair Credit Reporting Act, the Wiretap Act, and Illinois's Biometric Information Privacy Act all include a private right of action—a provision that authorizes affected or aggrieved individuals to sue entities that violate the law.[18]

Both conventional enforcement schemes have serious shortcomings. Public enforcement—which relies on a small number of government enforcers—is a rather rare phenomenon.[19] The FTC averages only about ten privacy cases each year.[20] In 2021, the FTC initiated six new cases that included a data privacy or cybersecurity allegation.[21] One involved illegal robocalls, one targeted a spyware developer, and one alleged violations of the Children's Online Privacy Protection Rule.[22] The rest alleged that a company violated its own privacy policy.[23] So the FTC's 2021 privacy cases amounted to little more than

15 *See, e.g.*, Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221 (2022).

16 *See, e.g.*, JAMES X. DEMPSEY, CHRIS JAY HOOFNAGLE, IRA S. RUBINSTEIN & KATHERINE J. STRANDBURG, BREAKING THE PRIVACY GRIDLOCK: A BROADER LOOK AT REMEDIES 5–6 (2021); Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 ME. L. REV. 15, 16 (2021).

17 *See infra* notes 153–56 (GDPR), 105–06 (CCPA), 101–02 (FTC) and accompanying text.

18 *See infra* notes 186–98 and accompanying text; *see also* 18 U.S.C. § 2520(a) (2018) (The Wiretap Act).

19 *See infra* subsection II.A.1.

20 ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 114 (2021).

21 *See* FED. TRADE COMM'N, CASES & PROCEEDINGS, https://ftc.gov/enforcement/cases-proceedings [https://perma.cc/WN6K-VYHQ] (database on file with author).

22 *See* Complaint paras. 1–17, FTC v. Associated Cmty. Servs., Inc., No. 21-cv-10174 (E.D. Mich. Jan. 26, 2021) (illegal robocalls); Complaint paras. 29, 31–34, *In re* Support King, LLC, No. C-4756 (F.T.C. Dec. 20, 2021) (spyware developer); Complaint paras. 36– 38, United States v. Kuuhuub Inc., No. 21-cv-01758 (D.D.C. June 30, 2021) (collecting and disseminating information from children without attempting to obtain parental consent).

23 *See* Complaint paras. 34–56, United States v. OpenX Techs., Inc., No. 21-cv-09693 (C.D. Cal. Dec. 15, 2021) (collecting location information from users who opted out and from children without attempting to obtain parental consent); Complaint paras. 13–26, *In*

singling out a handful of bad actors and holding a few companies to their own promises.

Even when governmental regulators act, the remedies they pursue tend to entrench rather than disrupt the status quo.[24] The FTC typically imposes auditing and assessment requirements on the companies it investigates, but these mandates rely almost exclusively on the businesses' own conclusory representations.[25] In rare instances where regulators impose financial penalties, the sums extracted are minuscule compared to the companies' profit-generating capacity.[26] Privacy law—as enforced by governmental regulators—is little more than a necessary cost of doing business.

Both ills with public enforcement could seemingly be cured by a private right of action: authorizing plaintiffs to sue promotes vigorous enforcement, and imposing statutory damages should shift incentives. And yet over the past generation, private enforcement has also proven increasingly ineffective due to court decisions on the enforceability of adhesion contracts, Article III standing, and class certification.[27]

Many companies use terms of service to impose a host of onerous restrictions on individuals' rights of redress, and the Supreme Court has been eager to enforce arbitration clauses that render claims infeasible to pursue in an individualized proceeding.[28] Even if a plaintiff avoids an arbitration clause, terms of service may nonetheless defeat a privacy claim on the merits by including a provision that says the user consented to the contested practices.[29] For example, both the Wiretap Act and Illinois's Biometric Information Privacy Act permit consent defenses.[30]

If the plaintiff can somehow avoid this pair of adhesion contract hurdles, she still must overcome a motion to dismiss that seizes on the Court's recent Article III standing decisions. The Court has repeatedly held that some intangible injuries are insufficiently "concrete" to invoke the jurisdiction of the federal courts, and privacy claims are particularly susceptible to intangible-injury arguments.[31] Only if the

re Flo Health, Inc., No. C-4747 (F.T.C. June 22, 2021) (sharing users' health information with third parties in violation of its privacy policy); Complaint paras. 5–22, *In re* Everalbum, Inc., No. C-4743 (F.T.C. May 7, 2021) (turning on facial recognition by default and failing to delete user data upon account deactivation, both in violation of its privacy policy).

24 *See infra* subsection II.A.2.

25 *See infra* notes 173–80 and accompanying text.

26 *See infra* notes 90, 181–83 and accompanying text.

27 *See infra* Section II.B.

28 *See infra* subsection II.B.1.

29 *See infra* subsection II.B.1.

30 *See* 18 U.S.C. § 2511(2)(c) (2018); 740 ILL. COMP. STAT. 14/15(d)(1) (2022).

31 *See infra* subsection II.B.2.

plaintiff makes a sufficiently strong analogy to a privacy tort from the mid-twentieth century will she keep her claim in federal court.[32]

But even if she does, the plaintiff will still need to run a gamut of difficult-to-satisfy criteria to have her class action certified. Many lower courts refuse to certify privacy class actions on an atextual consideration about whether the defendant's illegal practices are so complicated that it's too difficult to identify class members.[33] And the Supreme Court has also been enthusiastic about decertifying classes based on ever-heightening class certification requirements like commonality and predominance.[34]

In short, there are no fewer than a half-dozen significant obstacles that a privacy class action plaintiff must dodge and overcome before the action is economically feasible to pursue.

Contemporary debates about privacy law enforcement tend to outright ignore the uncomfortable reality that neither public nor private enforcement is effective at changing much of anything.[35] As Congress and statehouses debate new laws, industry allies insist on public enforcement because they know it will preserve the status quo.[36] On the other side of the aisle, most privacy advocates have focused on the private right of action—despite mounting evidence that only the unluckiest and least competent companies will be held accountable.[37]

This Article proposes a hybrid approach that solves the dichotomy between ineffective public enforcement and infeasible private enforcement: qui tam actions.[38] A qui tam is a legal action that authorizes a private plaintiff, called a relator, to redress an injury suffered by the government or by society, and successful relators are entitled to a portion of the recovery.[39] Qui tam has an ancient pedigree. English qui tam actions date to the thirteenth century, and the First Congress enacted a host of qui tam statutes shortly after the Framing.[40]

---

32 *See infra* notes 259–67 and accompanying text.

33 *See infra* subsection II.B.3.

34 *See infra* subsection II.B.3.

35 *See* COHEN, *supra* note 12, at 16.

36 *See, e.g.*, John Hendel & Cristiano Lima, *Lawmakers Wrangle over Consumer Lawsuits as Privacy Talks Drag*, POLITICO (June 5, 2019, 11:04 AM), https://politico.com/story/2019/06/05/privacy-advocates-consumer-lawsuits-1478824 [https://perma.cc/4H7P-JKJQ].

37 *See id.*; CAMERON F. KERRY, JOHN B. MORRIS, JR., CAITLIN T. CHIN & NICOL E. TURNER LEE, BROOKINGS INST., BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION 19 (2020); Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1654–55 (2022).

38 *See infra* Part III.

39 *See infra* notes 304–06 and accompanying text.

40 *See id.*

While a rarity today, some scholars have recently sought to resuscitate and resurrect the qui tam,[41] and it's easy to see why: qui tam is responsive to the shortcomings with both public enforcement and private enforcement. Authorizing private plaintiffs to bring a qui tam solves the underenforcement problem with governmental regulators, and relators are incentivized to seek significant damages rather than agree to toothless consent decrees.[42]

Relators' actions are also not subject to the same doctrinal obstacles as private suits. Relators can be exempt from onerous terms-of-service provisions—ensuring that suits remain in court and that blanket consent provisions don't defeat claims on the merits.[43] The Supreme Court has previously held that qui tam relators have Article III standing, so legislatures can empower relators to stand in the government's shoes to promote the public interest in the same way that an agency does.[44] Finally, because relators adopt the public enforcer's identity, there is no need for a qui tam to satisfy class certification criteria like ascertainability, commonality, and predominance.[45] The upshot is that a privacy qui tam is a powerful tool for addressing the significant shortcomings with conventional enforcement options.

Qui tam has historically been employed to vindicate collective injuries. Early American qui tam statutes prohibited fishing out of season and failing to return census reports.[46] So a crucial question about the viability of a privacy qui tam is whether violations of privacy law could plausibly be considered collective injuries amenable to qui tam enforcement.[47] Privacy in American law has long been considered an atomistic right that belongs to the individual.[48] So conceived, qui tam may seem like a rather odd fit: if businesses are violating individuals' privacy rights, can policymakers really employ a scheme that empowers the enforcer to remedy a public injury?

Fortunately, privacy scholars in recent years have convincingly shown that privacy should be understood as a social phenomenon that

41 *See, e.g.*, Myriam Gilles & Gary Friedman, *The New Qui Tam: A Model for the Enforcement of Group Rights in a Hostile Era*, 98 TEX. L. REV. 489, 491 (2020); Andrew Elmore, *The State Qui Tam to Enforce Employment Law*, 69 DEPAUL L. REV. 357, 359–60 (2020); Janet Cooper Alexander, *To Skin a Cat:* Qui Tam *Actions as a State Legislative Response to* Concepcion, 46 U. MICH. J.L. REFORM 1203, 1203 (2013); Zachary M. Dayno, *Private Citizens Policing Corporate Behavior: Using a* Qui Tam *Model to Catch Financial Fraud*, 43 VT. L. REV. 307, 311 (2018).

42 *See infra* subsection III.C.1.

43 *See id.*

44 *See infra* subsection III.C.2.

45 *See id.*

46 *See infra* subsection III.A.1.

47 *See infra* Section III.B.

48 *See, e.g.*, *infra* note 373 and accompanying text.

requires policy intervention at a structural level.[49] Privacy laws to date, however, have studiously avoided operationalizing these insights.[50] Current legal regimes fastidiously adhere to a notice-and-choice regime—one where individuals confronted with cumbersome dialog boxes and inscrutable terms of service are responsible for making wise decisions that protect their privacy.[51] This individualized and atomistic conception of privacy has helped produce the status quo, and any attempt to overcome the entrenchment of surveillance-based businesses must address this corroded foundation. Social theories of privacy illustrate that privacy is a crucial component of any free and open society and that a notice-and-choice regime ensures the steady degradation of a public value integral to human flourishing and democratic self-governance.[52] Qui tam enforcement is thus one piece of a larger puzzle about how to recast privacy law as responsive to the structural harms of information capitalism.

But merely invoking the qui tam label is no magic bullet. A California statute authorizes aggrieved employees to sue employers that violate California employment law on behalf of themselves and other aggrieved employees.[53] The law's qui-tam-like enforcement mechanism suffers from a series of grave defects—which have rendered it unnecessarily susceptible to private enforcement's shortcomings.[54] Future qui tam proposals must therefore learn from California's mistakes.[55]

This Article culminates in a detailed qui tam proposal that has the strongest possible chance of augmenting public enforcement without falling victim to private enforcement's pitfalls.[56] It's not too late for policymakers to recognize that repetition of the same formula will invariably produce the same results. This Article supplies those policymakers with a novel enforcement structure with deep roots and great promise.

This Article has three parts. Part I surveys recent developments in privacy law and reviews scholars' criticisms of these new legal regimes. Part II identifies the shortcomings with conventional enforcement schemes. Part III turns to qui tam. It first traces the qui tam through history and reviews a pair of prominent qui tam statutes that have provoked the Supreme Court's interest. Understanding this history—the

49 *See infra* subsection III.B.1.
50 *See* COHEN, *supra* note 12, at 3–8.
51 *See id.*; Waldman, *supra* note 6, at 35–40.
52 *See infra* subsection III.B.1.
53 *See* CAL. LAB. CODE § 2699(a) (West 2022).
54 *See infra* subsection III.A.2.
55 *See infra* subsections III.A.2 and III.C.2.
56 *See infra* subsection III.B.2.

Court's framework for analyzing qui tam actions and the perils others have faced—proves vital to proposing a privacy qui tam that is responsive to the shortcomings identified earlier.

I. PRIVACY LAW IN THEORY & IN PRACTICE

Recent years have witnessed a spate of new privacy laws in Europe and the United States. This Part recounts some of these developments and then surveys scholarly criticism of these laws' approaches.

A. Recent Developments

Privacy has received considerable attention from governments in Europe and the United States in recent years.

Ari Ezra Waldman has explained that we are in the midst of a second wave of privacy laws.[57] The first wave of privacy law is composed of "sector-specific federal statutes, Federal Trade Commission . . . consent decrees, and a default transparency requirement known as notice-and-consent."[58] First-wave privacy laws are characterized by "click-to-agree, opt-out consents, and long legalese privacy notices. Governance was self-regulatory and classically liberal."[59]

The second wave, Waldman shows, arrived in mid-2018 with the implementation of the European Union's GDPR and California's passage of the CCPA.[60] The GDPR is constructed "around the concept of 'lawful processing' of data," which means that, as a general matter, "personal data cannot be processed unless a data controller has obtained individual consent."[61] On top of this consent foundation, the law guarantees several privacy rights to European Union internet users, including the right to be notified about a security breach, the right to access information, the right to erasure, and the right to data portability, among others.[62]

The GDPR and the CCPA are similar in many respects. Both laws define personal information broadly and emphasize transparency; like the GDPR, the CCPA includes notice, access, portability, and opt-out

57 Waldman, *supra* note 6, at 21.

58 *Id.* at 22.

59 *Id.*

60 *See id.* at 21.

61 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1756 (2021) (citing GDPR, *supra* note 1, art. 6(1)(a)). In addition to individual consent, the GDPR enumerates five other categories of lawful processing. *See id.* (citing GDPR, *supra* note 1, arts. 6(1)(a)–(f)).

62 *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1908–09 (2019) (citing GDPR, *supra* note 1, arts. 33, 15, 17, 20, 16, 18, 21).

rights.[63] The CCPA, however, is more modest and lacks many of the major structural elements of the GDPR.[64] For example, the GDPR is more sweeping in the duties imposed and in the breadth of entities covered.[65]

The GDPR's effective date and the CCPA's passage triggered a torrent of additional privacy laws and proposals.[66] Waldman observes that the second wave's constituents are remarkably similar: "[T]hey combine a series of individual rights with internal compliance structures in which industry is its own privacy governor."[67] That's not to suggest, however, there is no difference between the first and second waves. The second wave "imposes more obligations on industry than the responsibility to write, post, and adhere to a privacy policy that no one reads," by adding requirements like privacy impact assessments, chief privacy officers, internal audits, self-certified compliance, paper trails, and internal processes for adjudicating consumer rights.[68]

The second wave continues unabated. In 2020, California voters approved a ballot initiative titled the California Privacy Rights Act (CPRA), and the CPRA expands and refines certain elements of the CCPA.[69] In 2021 and 2022, Virginia, Colorado, and Utah enacted new privacy laws modeled on the CCPA.[70] Several other states have enacted more modest proposals.[71] And many states continue to consider CCPA-style proposals, while about a dozen similar bills have been introduced in Congress.[72]

---

63 *See* Chander et al., *supra* note 61, at 1749–55.

64 *See id.* at 1746.

65 *See id.* at 1755–62.

66 *See* Waldman, *supra* note 6, at 21–22.

67 *Id.* at 22.

68 *Id.*

69 *See CCPA vs CPRA: What's the Difference?*, BLOOMBERG L. (July 13, 2021), https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ [https://perma.cc/9KW6-E7S9].

70 *See* Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, IAPP (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/ [https://perma.cc/F6UM-55MB]; Sarah Rippy, *Colorado Privacy Act Becomes Law*, IAPP (July 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/ [https://perma.cc/U7SJ-8AQV]; Taylor Kay Lively, *Utah Becomes Fourth US State to Enact Comprehensive Consumer Privacy Legislation*, IAPP (Mar. 25, 2022), https://www.iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/ [https://perma.cc/VWP5-KBUN].

71 *See supra* note 5 and accompanying text.

72 *See* Waldman, *supra* note 6, at 21 nn.2–3.

B. Criticisms

Privacy scholars are divided on the merits of this second wave of privacy law. Some have characterized the CCPA and its aftermath as a "paradigm shift."[73] Others have been less charitable. This Section reviews two distinct critiques: the first is an attack on the structure and ideology of second-wave laws; the second focuses on how the new laws are enforced.

1. Structure & Ideology

Several prominent privacy scholars have sought to conceptualize and taxonomize information capitalism's effects on our laws and institutions. These scholars have shed light on why changes in privacy law have had so little effect on businesses that extract and monetize personal information.

Julie E. Cohen has observed that the networked information age is effecting a transformation of law and legal institutions.[74] Cohen's argument is built on the foundational premise that the contours of our legal institutions are a response to contests over resources and the harms that arose during the industrial age.[75] As our political economy shifts from industrial to informational, law and legal institutions are attempting to respond to new contests over new resources and to new and different harms.[76]

Unfortunately, privacy law remains mired in the past. Cohen explains that both "existing information privacy laws and the recent crop of legislative proposals are pervasively informed by a governance paradigm that is deeply embedded in the U.S. legal tradition and that relies on individual assertion of rights to achieve social goals."[77] But the "rote, brute-force application of laws designed around the governance challenges of a prior era," she argues, "will not resolve the governance dilemmas created by today's surveillance-based business models."[78] Even the strongest privacy law suffers from a catastrophic defect: the GDPR "imposes a substantive duty of data protection by design and default, but it does not specify the sorts of design practices that such a

73 *See, e.g.*, Chander et al., *supra* note 61, at 1737; *see also* Margot E. Kaminski, *The Case for Data Privacy Rights (or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 399 (2022).

74 JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 1 (2019).

75 *See id.* at 2.

76 *See id.*

77 COHEN, *supra* note 12, at 3.

78 *Id.* at 2–3.

duty might require. There is a hole at the center where substantive standards ought to be . . . ."[79]

Ari Waldman has similarly taken a critical lens to new privacy laws and proposals. Despite the second wave's "veneer of protection," privacy law "is failing to deliver its promised protections in part because the corporate practice of privacy reconceptualizes adherence to privacy law as a compliance, rather than a substantive, task."[80] A managerial, neoliberal mindset pervades privacy law compliance—prioritizing "innovation over regulation, efficiency over social welfare, and paperwork over substance."[81] This mindset becomes self-reinforcing, "open[ing] the door for companies to create structures, policies, and protocols that comply with the law in name only."[82] As "these symbolic structures become more common," Waldman explains, "judges and policymakers defer to them as paradigms of best practices or as evidence for an affirmative defense or safe harbor, mistaking mere symbols of compliance with adherence to legal mandates."[83]

2. Enforceability

It's not only the ideology, structure, and compliance mechanisms that limit privacy law's effectiveness. Even privacy laws that hint at superior substantive provisions are threatened by an inability to enforce them effectively. Since the strongest data protection regulations have a gaping void at their center, "data protection regulators often rely on alleged disclosure violations as vehicles for their enforcement actions," continuing to rely on broken promises and unwelcome surprise as the path of least resistance.[84]

The conventional wisdom is that there are two strategies for pursuing information privacy violations: "private remedial litigation initiated by affected individuals and public enforcement action initiated by agencies."[85] Proposals that double down on one or both strategies, Julie Cohen argues, "tend to overlook the inconvenient truth that ex post, litigation-centered approaches have not proved especially effective at constraining Big Tech's excesses."[86]

Cohen levies two critiques at public and private litigation-centered approaches: "First, because enforcement litigation is predominantly atomistic in its identification and valuation of harms, it cannot

79 *Id.* at 13.
80 Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776 (2020).
81 *Id.* (citing COHEN, *supra* note 74, at 143–47).
82 *Id.* at 776–77.
83 *Id.* at 777.
84 COHEN, *supra* note 12, at 13.
85 *Id.* at 16 (citing KERRY ET AL., *supra* note 37).
86 *Id.*

effectively discipline networked phenomena that produce widely distributed, collective harms manifesting at scale."[87] Second, "enforcement litigation tends to . . . ha[ve] little to say about *how* violations ought to be remedied."[88] In other words, "when the challenged behavior is both highly profitable and relatively opaque to outside observers, it empowers violators to treat the costs of occasional enforcement actions as operating expenses."[89] The FTC's 2019 contempt order against Facebook starkly illustrates this second critique: in exchange for a stunningly broad liability release, Facebook paid the largest penalty ever levied by the FTC, which amounted to only a single month of the company's earnings.[90]

Scholars have sought to draw inspiration for novel enforcement mechanisms from fields outside traditional privacy and consumer protection regulation, like environmental law,[91] financial services,[92] and the common law.[93] Others have focused on understanding how companies are responding to current law: some have argued that core aspects of the modern web's surveillance infrastructure violate today's data protection laws,[94] while others have sought to identify the methods that corporate actors use to skirt compliance.[95]

There can therefore be little doubt that the enforcement mechanism is one of the most significant, controversial, and vital questions about the efficacy of privacy law. The next two Parts examine in detail the conventional options: public enforcement by a governmental regulator and private enforcement by individual plaintiffs.

---

87 *Id.* at 17.

88 *Id.*

89 *Id.*

90 *Id.* at 17–19; *see also* Dissenting Statement of Commissioner Rohit Chopra, *In re* Facebook, Inc., FTC Docket No. C-4365, at 17 (July 24, 2019) [hereinafter Chopra Dissent] ("I have not been able to find a single Commission order . . . that contains a release as broad as this one. The Commission is releasing both all known Section 5 claims *and* any and all order violation claims, whether known or unknown, concealed or disclosed." (footnote omitted)).

91 *See, e.g.*, DEMPSEY ET AL., *supra* note 16, at 19–23; Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 10 (2006).

92 *See, e.g.*, Sebastian Benthall & Salomé Viljoen, *Data Market Discipline: From Financial Regulation to Data Governance*, 8 J. INT'L & COMPAR. L. 459, 460 (2021); DEMPSEY ET AL., *supra* note 16, at 7–14; Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 485–88 (2020).

93 *See, e.g.*, Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 658 (2019); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614, 614 (2018); Ormerod, *supra* note 62, at 1927.

94 *See* Michael Veale & Frederik Zuiderveen Borgesius, *Adtech and Real-Time Bidding Under European Data Protection Law*, 23 GERMAN L.J. 226, 249 (2022).

95 *See* Helen Nissenbaum, Katherine Strandburg & Salomé Viljoen, *The Great Regulatory Dodge* (manuscript at 13) (on file with the *Notre Dame Law Review*).

II. CONVENTIONAL ENFORCEMENT'S SHORTCOMINGS

The vast majority of laws have one of two enforcement structures: either the law is exclusively enforced by one or more governmental regulators, or the law authorizes private individuals to enforce it. This Part examines the shortcomings with these conventional enforcement schemes.

A. Public Enforcement

Many laws are enforced by a governmental regulator.

Christian Turner has employed the public/private distinction to taxonomize legal systems.[96] He conceptualizes enforcement structures by asking: "who can 'call the question'—private parties or only the public? . . . The question is, again, based on power. Who can force adjudication?"[97] Identifying a law's enforcement structure asks: "How many enforcers should be given the responsibility for policing and preventing violations?"[98] With public enforcement, a "single administrative agency, such as the SEC, can be given an enforcement monopoly, and alternative enforcers, such as private class action lawyers, can be excluded."[99] Public enforcement can also be less centralized: multiple federal agencies and state attorneys general may be empowered to bring enforcement actions for violations of federal law.[100]

At the federal level, a prime example of public enforcement is the FTC's authority over unfair and deceptive acts or practices ("UDAP"). Immediately following the prohibition,[101] the Federal Trade Commission Act "empower[s] and direct[s]" the Commission to "prevent persons, partnerships, or corporations" from using "unfair or deceptive acts or practices in or affecting commerce."[102]

---

96 Christian Turner, *Law's Public/Private Structure*, 39 FLA. ST. U. L. REV. 1003, 1011–12 (2012). The other sorting criterion is whether a public or private actor is responsible for creating the law. *See id.* at 1010.

97 *Id.* at 1011.

98 Max Minzner, *Should Agencies Enforce?*, 99 MINN. L. REV. 2113, 2118 (2015).

99 *Id.*

100 *See id.*; Amy Widman & Prentiss Cox, *State Attorneys General's Use of Concurrent Public Enforcement Authority in Federal Consumer Protection Laws*, 33 CARDOZO L. REV. 53, 67–68 (2011); Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698, 699–704 (2011); Amanda Rose, *State Enforcement of National Policy: A Contextual Approach (with Evidence from the Securities Realm)*, 97 MINN. L. REV. 1343, 1345 (2013).

101 15 U.S.C. § 45(a)(1) (2018).

102 *Id.* § 45(a)(2). UDAP prohibitions aren't invariably enforced publicly. For example, California's unfair business practices statute previously conferred enforcement authority on any person acting in the public interest. *See* Ormerod, *supra* note 62, at 1928 (discussing 1977 Cal. Stat. 1202 (1993) (current version at CAL. BUS. & PROF. CODE § 17204 (West 2022)), which authorized a civil action to enforce Unfair Business Practices Act, CAL.

The FTC is a salient example of public enforcement because the FTC's "activities, often in the form of public settlement agreements with companies, form the most important regulation of information privacy in the United States."[103] Daniel J. Solove and Woodrow Hartzog have argued that the FTC's settlement agreements constitute a common law of privacy: through these settlements, the "FTC has codified certain norms and best practices and has developed some baseline privacy protections," and this "surprisingly rich" regulatory regime "focuses on consumer expectations of privacy, extends far beyond privacy policies, and involves a full suite of substantive rules that exist independently from a company's privacy representations."[104]

At the state level, the CCPA—both before and after being amended by the CPRA—is publicly enforced. As originally enacted, the CCPA vested most enforcement authority with the California Attorney General.[105] Following passage of the CPRA, enforcement authority is now vested with a new dedicated agency—the California Privacy Protection Agency.[106]

Outside of California, biometric privacy laws in Texas and Washington are exclusively enforced by those states' attorneys general.[107] And in addition to privacy-specific state statutes, state attorneys general have increasingly pursued companies engaged in abusive informational practices under state UDAP authority.[108]

Public enforcement of privacy law through an agency like the FTC or California Privacy Protection Agency faces a pair of significant challenges: public regulators only rarely bring enforcement actions, and their remedies tend to entrench the status quo.

1. Underenforcement

The first significant shortcoming with public enforcement of privacy law is that regulators bring enforcement actions very rarely.

BUS. & PROF. CODE § 17200 (West 2022), by "any person acting for the interests of itself, its members, or the general public").

103 CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY, at xiii (2016).

104 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014).

105 *See* Letter from Xavier Becerra, Cal. Att'y Gen., to Ed Chau, Cal. Assemb. and Robert M. Hertzberg, Cal. Sen. (Aug. 22, 2018) (on file with the *Notre Dame Law Review*) [hereinafter Becerra Letter]. The law does confer a limited private right of action on data breach victims. *See id.*

106 *See* CAL. CIV. CODE § 1798.199.10(a) (West 2022).

107 *See infra* note 198 and accompanying text.

108 *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 754 (2016).

The FTC's experience is instructive. The FTC initiated only six new privacy enforcement actions in 2021, and half were premised on the businesses' inaccurate or inadequate disclosures.[109] The previous year was no better.[110] Throughout the history of the FTC's regulation of privacy, "it has primarily pursued companies that break their promises in privacy notices and terms of service," and it "almost universally focuses on information industry behaviors that deceive individuals and create information asymmetries that undermine markets."[111] As Danielle D'Onfro puts it, "for a long time, the FTC just hasn't had the . . . wherewithal to bring complex cases;" it tends to "get hung up on petty little things" and ignores larger structural issues.[112]

What accounts for this meek and unimaginative regulatory strategy? Many have pointed to a lack of funding. The FTC is a small agency with an annual budget of about $300 million and a total staff of about 1,100—no more than fifty of which are tasked with privacy.[113] In contrast, the United Kingdom's privacy and data protection regulator has over 700 employees and a £38 million budget.[114] Germany's data protection agency has 745 staff, and France's nearly 200.[115] Given these constraints, the "FTC can only bring actions against a small fraction of infringers, and it has chosen cases wisely to make loud statements to industry about how to protect privacy."[116] On average, the FTC announces fewer than twenty deception and unfairness cases a year, and most UDAP cases don't implicate privacy.[117] One of the problems with selecting a small number of targets for maximum impact is that singling out only the most egregious actors "tends to validate the

109 *See supra* notes 20–23 and accompanying text.

110 *See* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2020 PRIVACY AND DATA SECURITY UPDATE 2–4 (2020).

111 WALDMAN, *supra* note 20, at 99.

112 Felipe Jimenez, *Danielle D'Onfro on Error-Resilient Consumer Contracts*, PRIV. L. PODCAST, at 11:50–12:37 (Mar. 18, 2021), https://anchor.fm/felipe-jimenez35/episodes/Danielle-DOnfro-on-Error-Resilient-Consumer-Contracts-esuj42 [https://perma.cc/FR8N-BBXN].

113 Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS: TECHTANK (Aug. 8, 2019) https://brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/2BH9-VJ34].

114 *Id.*

115 *See Protecting Consumer Privacy: Hearing Before the S. Comm. on Com., Sci. & Transp.*, 117th Cong. 3 (2021) (testimony of Ashkan Soltani, Independent Technologist) [hereinafter Soltani], https://commerce.senate.gov/services/files/5771F646–244C-4E39–8844-D0AEE1940E00 [https://perma.cc/W7YF-MJ7W].

116 Hoofnagle et al., *supra* note 113.

117 *See id.*

mainstream of current conduct rather than meaningfully shifting its center of gravity."[118]

The FTC's resource constraints operate across multiple dimensions. The Commission's Division of Privacy and Identity Protection is composed of about forty lawyers and fewer than ten technologists.[119] As the Commission's former Chief Technologist explained, having too few staffers "leads the agency to prioritize certain cases, and ignore privacy violations if they aren't deemed sufficiently harmful or easy to prosecute, or if the staff hours aren't available."[120] The Commission also has limited enforcement staff to monitor companies' compliance with consent decrees, and the Division of Enforcement—which is distinct from the privacy division—oversees every consent decree.[121] So the "same lawyers who ensure that social media companies have robust privacy and data security programs are making sure labels on bed linens are correct."[122]

It surely is true that the FTC would be capable of bringing more enforcement actions if it were appropriated more money. But the FTC's funding woes are merely a symptom of a larger phenomenon that also produces underenforcement. The underlying cause is stiff opposition to robust consumer protection among the regulated businesses and among the lawmakers who are politically accountable to those business interests. The FTC's lack of resources and the resulting dearth of enforcement actions are thus both downstream consequences of two intertwined forces: regulatory capture and industry's sway with the politicians that oversee the FTC.

Regulatory capture occurs when a policymaker or regulator is coopted to serve the interests of a minor—but organized and motivated—constituency. While much agency enforcement occurs outside of public attention, "the community regulated by the agency keeps a close eye on agency enforcement at all times," since they, after all, "pay the penalties that the agency imposes."[123] The regulated community "can easily affect enforcement choices (or other agency decisions) through its influence over Congressional oversight, activity that falls under the broad label of regulatory capture."[124] Capture "has become recognized as one of the central impediments to optimal policy regimes,"[125] and there is a rich legal literature on regulatory capture and

118 COHEN, *supra* note 12, at 17.
119 Soltani, *supra* note 115, at 3.
120 *Id.*
121 *Id.* at 3–4.
122 *Id.* at 4.
123 Minzner, *supra* note 98, at 2137.
124 *Id.*
125 *Id.*

public enforcement.[126] Several scholars have argued that federal administrative agencies are particularly vulnerable to capture because they "regulate highly organized sectors of the economy with deep pockets."[127]

A very slight remove from politics is encoded into the FTC's design: the Commission is led by five political appointees, three of which—including the chair—are from the President's political party.[128] In the case of the FTC's 2019 settlement with Facebook, both Democratic commissioners vociferously dissented from the terms of the agreement the Commission reached with the company.[129] The two Democratic commissioners argued that the penalty was insufficient, the liability release was too broad, the injunctive relief was unlikely to change anything, and that the Commission should have pursued personal liability for Facebook's directors and officers.[130] Despite high-profile Republican criticism of Facebook,[131] the FTC settlement shows that the Republican party's probusiness and antiregulation commitments often prevail over widespread antipathy for the company.

But the underenforcement of privacy law cannot be blamed exclusively on Republicans. Both Texas and Washington have biometric privacy laws that are only enforceable through those states' attorneys general.[132] Texas's attorney general has been a Republican for over two decades and Washington's has been a Democrat since 2013.[133] Between them, Texas has initiated only a single enforcement action under its biometric privacy law.[134]

---

126 *See id.*; Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 COLUM. L. REV. 1260, 1284 (2006); Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 TEX. L. REV. 15, 22 (2010); Lemos, *supra* note 100, at 717; Rose, *supra* note 100, at 1386.

127 Minzner, *supra* note 98, at 2137–38.

128 *See Commissioners*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/commissioners [https://perma.cc/3BLU-F789].

129 *See* Chopra Dissent, *supra* note 90, at 4; Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In re* Facebook, Inc., FTC Docket No. C-4365, at 2 (July 24, 2019) [hereinafter Slaughter Dissent].

130 *See* Chopra Dissent, *supra* note 90, at 12–20; Slaughter Dissent, *supra* note 129, at 6–15.

131 *See, e.g.*, Emily Stewart, *Silicon Valley Should Take Josh Hawley's Big War on Big Tech Seriously*, VOX (Oct. 29, 2019, 6:30 AM), https://vox.com/recode/2019/10/29/20932064/senator-josh-hawley-tech-facebook-google-mark-zuckerberg-missouri [https://perma.cc/RJ3K-7ZH2].

132 *See infra* note 198 and accompanying text.

133 *See Texas Attorney General*, WIKIPEDIA, https://wikipedia.org/wiki/Texas_Attorney_General [https://perma.cc/MX4R-RKEQ]; *Attorney General of Washington*, WIKIPEDIA, https://wikipedia.org/wiki/Attorney_General_of_Washington [https://perma.cc/3KP5-N9DG].

134 *See* Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 118 (2019). *See generally* Cecilia Kang, *Texas*

There is, in other words, bipartisan consensus that favors weak enforcement, and this has long been true for the FTC too. For much of its modern history, "Congress has kept the FTC on a short leash."[135] Lawmakers have "held authorization over the agency's head and used oversight power to scrutinize what members of Congress perceive as the expansive use of FTC legal authority, including its interpretation of privacy harm."[136]

The FTC's failed attempt to regulate advertising directed at children in the 1970s illustrates the extremely difficult environment that robust consumer protection faces. Spurred by concerns about sugar-filled foods and vitamin advertising that ran during the Saturday morning cartoon marathon, the FTC proposed to regulate these advertisements under the Commission's unfairness authority.[137]

The proposal provoked significant backlash from industry and Congress, and this controversy—known as KidVid—played a central role in the 1980 shutdowns of the Commission.[138] KidVid "still has a powerful psychological effect on the Agency," and the episode is often invoked "as a kind of threat that Congress will neuter the Agency if it takes the wrong action."[139] Congress reacted by passing the Federal Trade Commission Improvement Act of 1980.[140] Even though the law did little to alter the FTC's powers, "the substance and procedure of the act's passage did much political and psychological damage to the Agency."[141] The backlash illustrates that "business interests had become much more disciplined in organizing against federal regulation and regulators."[142]

Luke Herrine has argued that the FTC since KidVid embodies the profound influence of the neoliberal framework.[143] Neoliberalism posits that "human well-being can best be advanced by the maximization of entrepreneurial freedoms within an institutional framework

---

Sues Facebook's Parent, Saying It Collected Facial Recognition Data Without Consent., N.Y. TIMES (Feb. 14, 2022), https://nytimes.com/2022/02/14/technology/texas-facebook-facial-recognition-lawsuit.html [https://perma.cc/AVD9-ZMA7].

135 Hoofnagle et al., *supra* note 113.

136 *Id.*

137 HOOFNAGLE, *supra* note 103, at 60.

138 *See id.* at 60–66. These episodes were "probably the first time an agency has been shut down over a policy matter." *See id.* at 65 (citing J. HOWARD BEALES, III, ADVERTISING TO KIDS AND THE FTC: A REGULATORY RETROSPECTIVE THAT ADVISES THE PRESENT 8 (2004)).

139 *Id.* at 60.

140 *Id.* at 65 (citing Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980)).

141 *Id.*

142 *Id.* at 65–66.

143 *See* Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 431 (2021).

characterized by private property rights, individual liberty, unencumbered markets, and free trade."[144] But since markets are not self-sustaining—"they tend toward monopoly, destructive extraction, and rent-seeking"—neoliberal governmentality "resolves that embedded contradiction by bringing market dynamics and associated managerial techniques into government, infusing processes of legal and regulatory oversight with a competitive and capitalist ethos."[145]

Herrine argues that—contrary to KidVid's conventional overreach narrative—the Commission's regulatory initiatives in the 1970s were quite popular with the public, but they catalyzed radicalization among the leaders of businesses whose profits were threatened.[146] These business leaders became increasingly "well-organized and brought their new political clout to bear on an unsuspecting FTC."[147] Herrine contends that it wasn't "the re-articulation of the unfairness standard in 1980 that narrowed unfairness to its current form, but rather the subsequent takeover of the FTC by neoliberal economists and lawyers who had been supported by these radicalized business leaders."[148]

While some recent developments suggest the FTC is newly emboldened,[149] industry opposition and the authority of industry's political clients continue to stalk the Commission's organization and regulatory strategy. The FTC's former Chief Technologist has explained that "due to political pressures, [the Commission's] technologists were housed not as a separate division that could serve the entire agency, but instead in an obscure business unit within the IT staff."[150] This awkward and hobbled structure is still in place today, and it dramatically limits technologists' influence across the Commission.[151] Others have also explained that the FTC has simply declined to use many of

144 COHEN, *supra* note 74, at 7 (quoting David Harvey, *Neoliberalism as Creative Destruction*, 610 ANNALS AM. ACAD. POL. & SOC. SCI. 22, 22 (2007)).

145 *Id.* (citing Nicholas Gane, *The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and Beyond*, 60 SOCIO. REV. 611, 625–29 (2012)).

146 Herrine, *supra* note 143, at 433.

147 *Id.*

148 *Id.*

149 *See Trade Regulation Rule on Commercial Surveillance*, OFF. OF INFO. & REGUL. AFFS., EXEC. OFF. OF PRESIDENT, https://reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69 [https://perma.cc/GK29-L5SC]; *FTC Signals It May Conduct Privacy, AI, & Civil Rights Rulemaking*, ELEC. PRIV. INFO. CTR. (Dec. 10, 2021), https://epic.org/ftc-signals-it-may-conduct-privacy-ai-rulemaking/ [https://perma.cc/C7VW-XHGA].

150 Soltani, *supra* note 115, at 5.

151 *Id.*

the statutory authorities that Congress has already conferred on the Commission.[152]

The neoliberal framework and the resulting capture operate overseas too. Under the GDPR's "one stop shop" mechanism, for example, most enforcement authority belongs to the governmental regulator in the country where a company has its European headquarters,[153] and many technology companies have opted for oversight by Ireland or Luxembourg.[154] Privacy advocates blame this enforcement bottleneck for the GDPR's underwhelming enforcement record.[155] These countries have actively courted technology companies using a "mix of low corporate tax rates and business-friendly regulation," and these "close relationships have created a strong degree of economic dependency."[156] Informational businesses have thus been extremely effective at neutralizing the small number of relevant European regulators.

There are, nevertheless, some promising signs that data privacy regulation could become more serious. Following the CCPA's passage, the California Attorney General urged the California legislature to authorize a private right of action, arguing: "The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office]'s need for new enforcement resources."[157] While the legislature disregarded the request, the 2020 ballot initiative—the CPRA—siphoned some enforcement authority from the attorney general to a new dedicated agency.[158] The California Privacy Protection Agency's

152 *See* ELEC. PRIV. INFO. CTR., WHAT THE FTC COULD BE DOING (BUT ISN'T) TO PROTECT PRIVACY: THE FTC'S UNUSED AUTHORITIES 4–20 (2021).

153 *See* Annika Sponselee & Rodney Mhungu, *GDPR Top Ten #10: One Stop Shop*, DELOITTE, https://deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html [https://perma.cc/5MED-6EHS].

154 *See* Matt Burgess, *Why Amazon's £636m GDPR Fine Really Matters*, WIRED (Aug. 4, 2021, 6:00 AM), https://wired.co.uk/article/amazon-gdpr-fine [https://perma.cc/FHF7-8T2U].

155 *See, e.g.*, Natasha Lomas, *Ireland's Draft GDPR Decision Against Facebook Branded a Joke*, TECHCRUNCH (Oct. 13, 2021, 3:25 PM), https://techcrunch.com/2021/10/13/irelands-draft-gdpr-decision-against-facebook-branded-a-joke/ [https://perma.cc/S7WY-88G2]; Vincent Manancourt & Laura Kayali, *France Flexes Muscles with Fines Against Facebook, Google over Cookie Banners*, POLITICO (Jan. 6, 2022, 8:14 PM), https://politico.eu/article/france-takes-bite-out-of-cookie-banners-with-fines-targeting-facebook-google/ [https://perma.cc/8H6Y-9MEF].

156 Vinocur, *supra* note 11; *cf.* Stephanie Bodoni, *Silicon Valley's Top Privacy Cop Rejects Claims She's Too Lax*, BLOOMBERG (Nov. 18, 2021, 9:14 AM), https://bloomberg.com/news/articles/2021–11-18/eu-privacy-enforcement-not-good-enough-top-official-warns [https://perma.cc/SYH9-G7DY].

157 *See* Becerra Letter, *supra* note 105, at 2.

158 *See* CAL. CIV. CODE § 1798.199.10(a) (West 2022); *see also* Lydia de la Torre & Glenn Brown, *What Is the California Privacy Protection Agency?*, IAPP (Nov. 23, 2020), https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/ [https://perma.cc/ZW4Y-43H4].

enforcement authority does not begin until July 2023, and its $10 million annual budget pales in comparison to the staggering wealth of the industry it regulates.[159] So it remains to be seen whether the California Privacy Protection Agency, "a small $10m/year agency staffed with 50–60 personnel," can "effectively protect the privacy rights of 40 million Californians" against powerful companies whose business models are "predicated on surveilling and processing the personal information of those 40 million people."[160]

In sum, underenforcement of privacy law by agencies is a widely observed and well-documented phenomenon. The underlying causes of underenforcement are complex and contested, but it suffices to say that industry opposition—and the authority of the politicians in industry's thrall—has significant explanatory power over both the dearth of resources and the lack of robust enforcement.

2. Ineffective Remedies

A second shortcoming with public enforcement is the ineffectiveness of the remedies that agencies impose. Even if agency enforcement actions were commonplace, there's good reason to doubt that their outcomes would have a material effect on informational enterprises.

The FTC's authority to assess penalties is severely limited.[161] Only after a company violates an earlier settlement or injunction can the Commission extract fines.[162] The Supreme Court has also recently held that the FTC lacks the statutory authority to obtain equitable monetary remedies like restitution and disgorgement,[163] and Congress has shown little interest in revisiting that holding.[164]

Other agencies have broader authority to impose monetary penalties,[165] but they have suffered from the same defect as the FTC's 2019 Facebook settlement: the penalties pale in comparison to the

159 *See* Tom Kemp, *How the California Privacy Protection Agency Can Better Protect Consumers*, GOLDEN DATA (Oct. 14, 2021), https://medium.com/golden-data/how-the-california-privacy-protection-agency-can-better-protect-consumers-d7c33e9b0337 [https://perma.cc/XHU5-36CN]; *Frequently Asked Questions (FAQs)*, CCPA, https://cppa.ca.gov/faq.html [https://perma.cc/3SR3-QCW9].

160 *See* Kemp, *supra* note 159.

161 *See* Waldman, *supra* note 80, at 806 n.212 (first citing HOOFNAGLE, *supra* note 103, at 166; and then citing Solove & Hartzog, *supra* note 104, at 605).

162 *See* Solove & Hartzog, *supra* note 104, at 605.

163 *See* AMG Cap. Mgmt., LLC, v. FTC, 141 S. Ct. 1341, 1344 (2021).

164 *See, e.g.*, Justin Brookman (@JustinBrookman), TWITTER (May 11, 2022, 11:08 AM), https://twitter.com/JustinBrookman/status/1524406203098738689 [https://perma.cc/D45D-7W67].

165 *See, e.g.*, Chander et al., *supra* note 61, at 1759 (explaining the GDPR and CCPA penalty structures).

businesses' profit-generating capacity. The largest GDPR penalty announced to date was levied against Amazon and totaled €746 million.[166] No one really knows what provoked the fine and it's likely it will eventually be reduced.[167] And yet in the same quarter that the penalty was announced, Amazon earned $6.3 billion in profit—a performance that "badly misse[d]" expectations.[168] The record GDPR penalty before Amazon's was a paltry €50 million assessed against Google.[169]

Given that the FTC can only rarely assess penalties, the Commission's remedies take the form of specific performance. Daniel Solove and Woodrow Hartzog have explained that the FTC has used its deception and unfairness authority to forge a common law of privacy, and this common law is articulated through voluntary settlements with companies.[170]

While some have cast these settlements in a favorable light, others don't share their optimism. Julie Cohen, for example, explains that "public agencies have largely acquiesced in the emergence of conventions for structuring consent decrees that delegate most oversight to private auditors and in-house compliance officers."[171] Under these consent decrees, a "few additional managerial controls are imposed; additional consumer disclosures are incorporated into the already-existing documents that most consumers do not read; and the necessary reports are generated, reviewed by auditors, and filed with regulators."[172]

Ari Waldman has sought to comprehensively investigate the on-the-ground reality about what companies do to comply with these consent decrees. His findings are troubling. Based on original primary source research, he has found that privacy law is "failing to deliver its promised protections in part because the corporate practice of privacy

166 Burgess, *supra* note 154.

167 *See id.*

168 *See* Todd Spangler, *Amazon Misses Q3 Financial Expectations, Warns of Billions in Additional Costs in Year-End Quarter*, VARIETY (Oct. 28, 2021, 1:10 PM), https://variety.com/2021/digital/news/amazon-q3–2021-earnings-miss-1235099669/ [https://perma.cc/2KKS-JLNU]; Annie Palmer, *Amazon Badly Misses on Earnings and Revenue, Gives Disappointing Fourth-Quarter Guidance*, CNBC (Oct. 28, 2021, 8:15 PM), https://cnbc.com/2021/10/28/amazon-amzn-earnings-q3–2021.html [https://perma.cc/2V43-F2AW].

169 *See The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, EUR. DATA PROT. BD. (Jan. 21, 2019), https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en [https://perma.cc/S9W3-EP3G]; *Google Set for Record $50 Million GDPR Fine*, ADVANTAGE, https://www.advantage.co.uk/intelligence-hub/check-the-tech/google-set-for-record-50-million-gdpr-fine [https://perma.cc/TR2X-R8WH].

170 *See* Solove & Hartzog, *supra* note 104, at 585–86.

171 *See* COHEN, *supra* note 12, at 17 (citing COHEN, *supra* note 74, at 186–93; Waldman, *supra* note 80).

172 COHEN, *supra* note 74, at 162.

reconceptualizes adherence to privacy law as a compliance, rather than a substantive, task."[173] The FTC requires companies operating under consent decrees to regularly submit privacy assessments.[174] These assessments must be completed by a "'qualified, objective, independent third-party' auditor with sufficient experience," and "they must describe specific privacy controls, evaluate their adequacy given the size and scope of the company, explain how they meet FTC requirements, and certify they are operating effectively."[175]

Even though these assessments "are often the only real weapons in the FTC's arsenal because they ostensibly require a qualified, independent third party to verify corporate compliance," the reality is a vacuous and futile exercise.[176] Assessment conclusions "are based on assertions from management rather than wholly independent analyses from auditors, and are usually framed by goals set by management."[177] In other words, "the company that is supposed to be the subject of the assessment is, in fact, determining the bases upon which it gets evaluated, thus giving companies some power to predetermine the results."[178]

Waldman uses Google's FTC consent decree as an illustration of this dynamic. The FTC wanted, among other things, an assessment that ensured the company had a privacy team, an ongoing and flexible privacy assessment process, and relationships with vendors capable of protecting data.[179] Even if we were to accept that those conditions amounted to much—a dubious premise—the report's conclusion that Google was meeting the terms of its agreement were based exclusively on the company's own representations.[180] Fulfilling the requirements of the FTC's consent decrees is thus not just meaningless; it actively entrenches business practices that threaten privacy.

Facebook provides another revealing example of the consent decree's efficacy. The only reason the FTC was able to extract its $5 billion penalty in 2019 was because the company had entered a consent decree with the Commission in 2011.[181] The central tenet of that 2011 settlement? The same type of vaporous audits and assessments.[182]

173 Waldman, *supra* note 80, at 776.

174 *See id.* at 806 & nn.208–11.

175 *Id.* at 806 (quoting Decision and Order, *In re* Google Inc., FTC Docket No. C-4336 (Oct. 13, 2011)).

176 *Id.* at 806–07 (footnote omitted).

177 *Id.*

178 *Id.* at 807.

179 *Id.*

180 *Id.*

181 *See* Agreement Containing Consent Order, *In re* Facebook, Inc., FTC Docket No. C-4365 (Nov. 29, 2011).

182 *See id.* §§ IV–VI.

Facebook violated the terms of the 2011 consent decree in a dizzying list of ways,[183] which strongly suggests that the earlier settlement accomplished little more than laying the predicate for the later penalty.

* * *

Public enforcement vests authority with one or a few governmental regulators and doing so has clear and widely observed drawbacks: these agencies and enforcers face stiff headwinds in the form of appropriations, politics, and coordinated opposition among their targets, and even when they succeed, the net benefit of doing so is questionable. The next Section turns to public enforcement's conventional alternative.

B. Private Enforcement

In contrast to public enforcement, some laws confer enforcement authority on nongovernmental actors.

The term "private attorney general" may refer to several different things,[184] but as used throughout this Article, the term "private enforcement" is concerned with "private attorneys whose work for private clients contributes to the public interest by supplementing the government's enforcement of laws and public policies."[185] At the federal level, examples of laws that authorize private enforcement include the Fair Credit Reporting Act (FCRA) and the Telephone Consumer Protection Act (TCPA). The FCRA is "America's first federal consumer information privacy law and one of the first information privacy laws in the world."[186] The law is very complex and has been repeatedly amended, but briefly, the law "comprehensively regulate[s] consumer reporting and the practice of assembling files about consumers in order to evaluate them for credit, employment, tenancy, 'consumer-initiated' transactions, or other opportunities."[187] The FCRA principally

183 *See* Complaint for Civil Penalties, Injunction, and Other Relief paras. 35–190, United States v. Facebook, Inc., 456 F. Supp. 3d 115 (D.D.C. 2020) (No. 19-cv-2184); *see also* Chopra Dissent, *supra* note 90, at 17–18 (discussing conduct not enumerated in the 2019 settlement). A whistleblowing complaint filed with the Securities and Exchange Commission by Twitter's former head of security further confirms that the FTC's consent decrees are toothless and easily flouted. *See* Cat Zakrzewski & Joseph Menn, *Twitter Whistleblower Exposes Limits of FTC's Power*, WASH. POST (Sept. 12, 2022, 4:40 PM), https://www.washingtonpost.com/technology/2022/09/12/mudge-twitter-ftc-consent-decrees/ [https://perma.cc/ZXW5-B49N].

184 *See* William B. Rubenstein, *On What a "Private Attorney General" Is—and Why It Matters*, 57 VAND. L. REV. 2129, 2142 (2004).

185 *See id.* at 2146.

186 HOOFNAGLE, *supra* note 103, at 270.

187 *Id.* at 270, 275.

authorizes the FTC to enforce its requirements,[188] but also provides for a private right of action.[189]

The TCPA was a response to widespread outrage about the proliferation of robocalls and abusive telemarketing practices.[190] The law "effectively regulates these abuses by prohibiting certain technologies altogether, rather than focusing specifically on the content of the messages being delivered."[191] The TCPA is enforceable by a host of entities: the Federal Communications Commission has principal enforcement authority, though the law requires some consultation with the FTC;[192] the law also authorizes enforcement by state attorneys general;[193] and it creates a private right of action.[194] But one enforcer stands out among the rest: "Private parties have largely been responsible for enforcement of the Telephone Consumer Protection Act."[195]

At the state level, Illinois's Biometric Information Privacy Act (BIPA) is a recent privacy law with the private right of action. BIPA prohibits private entities from collecting certain biometric information unless the entity obtains written consent from the subject and supplies the subject with a written privacy policy that includes several specific disclosures, including the purpose of the collection and details about how the data will be secured.[196] The statute includes a private right of action, and it does not explicitly confer enforcement authority on any governmental entity.[197] In contrast and as noted above, biometric privacy laws in Texas and Washington do not include private rights of action and instead confer enforcement authority exclusively on the state attorney general.[198]

Including a private right of action is a seemingly simple solution to the shortcomings with public enforcement identified in subsection II.A.1. But the reality is far more complex: over the past thirty years,

188 *See* 15 U.S.C. § 1681s(a)(1) (2018).

189 *See id.* § 1681n(a); *see also* Spokeo, Inc. v. Robins, 578 U.S. 330, 335 (2016).

190 *See* Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335, 2344 (2020); Spencer Weber Waller, Daniel B. Heidtke & Jessica Stewart, *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology*, 26 LOY. CONSUMER L. REV. 343, 347 (2014).

191 Waller et al., *supra* note 190, at 347.

192 *See* 47 U.S.C. § 227(h)(1) (2018).

193 *See id.* § 227(e)(6); *see also* Widman & Cox, *supra* note 100, at 56.

194 *See* 47 U.S.C. § 227(b)(3) (2018); *see also, e.g.*, Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 461–62 (7th Cir. 2020).

195 Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 70 (2021) (internal brackets omitted) (quoting Waller et al., *supra* note 190, at 375).

196 *See* 740 ILL. COMP. STAT. 14/15(b) (2022); 740 ILL. COMP. STAT. 14/10 (2022).

197 740 ILL. COMP. STAT. 14/20 (2022).

198 *See* TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2021); WASH. REV. CODE § 19.375.030(2) (2022).

the Supreme Court has sharply limited individual plaintiffs' ability to vindicate legal rights conferred on them by Congress. This Section details three doctrines that form a complex web of obstacles that make private enforcement infeasible or impossible: adhesion contracts, Article III standing, and class action certification under Federal Rule of Civil Procedure 23.

1. Adhesion Contracts

A first significant shortcoming with relying on private rights of action is their vulnerability to adhesion contracts. This shortcoming manifests in two distinct ways—compelled arbitration and terms-of-service consent.

The first manifestation of this shortcoming concerns the Supreme Court's interpretation of the Federal Arbitration Act (FAA). The FAA provides in relevant part that a "contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[199]

In recent years, the Supreme Court has repeatedly interpreted the FAA expansively. In *Green Tree Financial Corp.-Alabama v. Randolph*, the Court granted the defendant's motion to compel arbitration, despite the plaintiff's argument that her statutory claim of a Truth in Lending Act violation would be difficult or impossible to pursue in arbitration.[200] The Court accepted that "the existence of large arbitration costs could preclude a litigant such as [the plaintiff] from effectively vindicating her federal statutory rights in the arbitral forum."[201] And yet the Court held that the plaintiff had failed to make that specific showing, so she was bound to arbitrate.[202]

Despite repeatedly recognizing this effective-vindication rule in theory, the Court has never used the rule to invalidate an arbitration clause.[203] The Court has said that the rule "would certainly cover a provision in an arbitration agreement forbidding the assertion of certain statutory rights," and "would perhaps cover filing and administrative fees attached to arbitration that are so high as to make access to the forum impracticable."[204] But absent those egregious

199 9 U.S.C. § 2 (2018).

200 Green Tree Fin. Corp.-Ala. v. Randolph, 531 U.S. 79, 90, 92 (2000).

201 *Id.* at 90.

202 *Id.* at 90–92.

203 *See, e.g.*, Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 637 n.19 (1985); 14 Penn Plaza LLC v. Pyett, 556 U.S. 247, 273–74 (2009); Gilmer v. Interstate /Johnson Lane Corp., 500 U.S. 20, 28 (1991).

204 Am. Express Co. v. Italian Colors Rest., 570 U.S. 228, 236 (2013).

circumstances, "the fact that it is not worth the expense involved in *proving* a statutory remedy does not constitute the elimination of the *right to pursue* that remedy."[205]

In *AT&T Mobility LLC v. Concepcion*, the Court confronted a California state-contract-law rule that held most class waivers in consumer arbitration agreement unconscionable.[206] Despite the FAA's savings clause specifically permitting generally applicable contract-law defenses like unconscionability, the Court held that the FAA preempted California's rule.[207] The Court reasoned that the "overarching purpose of the FAA . . . is to ensure the enforcement of arbitration agreements according to their terms so as to facilitate streamlined proceedings. Requiring the availability of classwide arbitration interferes with fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA."[208]

More recently, the Court has held that even when the FAA arguably conflicts with—and undeniably frustrates the objectives underlying—a later-in-time statute, the FAA prevails.[209] In *Epic Systems Corporation v. Lewis*, the Court rejected the employees' argument that enforcing mandatory individualized arbitration clauses in their employment contracts violated the National Labor Relations Act.[210] The Court's analysis has led scholars to question whether Congress can implicitly modify the FAA's applicability or whether only explicit arbitration carve-outs would be effective.[211]

Scholars and commentators have harshly criticized the Court's FAA jurisprudence. Many have questioned the Court's blithe and repetitious exhortation that the FAA reflects a "liberal federal policy favoring arbitration."[212] In addition to showing that the Court gets the history wrong, scholars have highlighted the practical effects of the Court's FAA cases. Janet Cooper Alexander, for example, explains that

---

205 *Id.*

206 AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 340 (2011) (explaining Discover Bank v. Superior Ct., 113 P.3d 1100 (Cal. 2005)).

207 *See id.* at 352.

208 *Id.* at 344.

209 *See* Epic Sys. Corp. v. Lewis, 138 S. Ct. 1612, 1623–29 (2018); *id.* at 1646 (Ginsburg, J., dissenting).

210 *See id.* at 1623–29 (majority opinion).

211 *See, e.g.*, David L. Noll, *Arbitration Conflicts*, 103 MINN. L. REV. 665, 707–28 (2018).

212 AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 339 (2011) (quoting Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 24 (1983)). For the scholars questioning this premise, see, for example, Rhonda Wasserman, *Legal Process in a Box, or What Class Action Waivers Teach Us About Law-making*, 44 LOY. U. CHI. L.J. 391, 399–407 (2012); Hiro N. Aragaki, *Equal Opportunity for Arbitration*, 58 UCLA L. REV. 1189 (2011); Katherine Van Wezel Stone, *Rustic Justice: Community and Coercion Under the Federal Arbitration Act*, 77 N.C. L. REV. 931 (1999).

after *Concepcion*, "if a party with power to dictate the terms of a contract chooses to eliminate access to courts or to aggregative proceedings, states are essentially powerless to protect the other party." [213] Myriam Gilles and Gary Friedman have argued both before and after *Concepcion* that "many—indeed, most—of the companies that touch consumers' day-to-day lives can and will now place themselves beyond the reach of aggregate litigation."[214] And given the small-dollar awards available in cases like *Green Tree* and *Concepcion*, successfully avoiding class actions means that few claims will be pursued—assuring immunity for schemes that cheat vast numbers of people out of individually small amounts of money.[215] Scholars have argued that the emptiness of the effective-vindication rule threatens legislatures' ability to enforce important public policies,[216] and others have demonstrated that recent decisions have spurred more companies to include mandatory individualized arbitration clauses in their terms of service.[217]

All of this, of course, bodes poorly for privacy law. Companies like Shutterfly and Snapchat have seized the opportunity to immunize themselves from BIPA class actions using terms-of-service arbitration clauses, and federal courts have granted both companies' motions to compel individualized arbitration.[218] Credit reporting companies have successfully used the same tactic to evade FCRA class actions.[219]

---

213 Alexander, *supra* note 41, at 1204.

214 Myriam Gilles & Gary Friedman, *After Class: Aggregate Litigation in the Wake of* AT&T Mobility v Concepcion, 79 U. CHI. L. REV. 623, 627 (2012) (citing Myriam Gilles, *Opting Out of Liability: The Forthcoming, Near-Total Demise of the Modern Class Action*, 104 MICH. L. REV. 373, 425–27 (2005)).

215 *See, e.g.*, Szetela v. Discover Bank, 118 Cal. Rptr. 2d 862, 868 (Cal. Ct. App. 2002) ("By imposing [an individualized arbitration] clause on its customers, [the defendant] has essentially granted itself a license to push the boundaries of good business practices to their furthest limits, fully aware that relatively few, if any, customers will seek legal remedies, and that any remedies obtained will only pertain to that single customer without collateral estoppel effect. The potential for millions of customers to be overcharged small amounts without an effective method of redress cannot be ignored."), *abrogated by Concepcion*, 563 U.S. 333.

216 *See, e.g.*, Olga Bykov, Note, *Vindication of Federal Statutory Rights: The Future of Cost-Based Challenges to Arbitration Clauses After* American Express v. Italian Colors Restaurant *and* Green Tree v. Randolph, 50 U.C. DAVIS L. REV. 1323 (2017); Einer Elhauge, Essay, *How* Italian Colors *Guts Private Antitrust Enforcement by Replacing It with Ineffective Forms of Arbitration*, 38 FORDHAM INT'L L.J. 771 (2015).

217 *See, e.g.*, Elizabeth C. Tippett & Bridget Schaaff, *How* Concepcion *and* Italian Colors *Affected Terms of Service Contracts in the Gig Economy*, 70 RUTGERS U. L. REV. 459 (2018).

218 *See* Miracle-Pond v. Shutterfly, Inc., No. 19 cv 04722, 2020 WL 2513099, at *1 (N.D. Ill. May 15, 2020); K.F.C. by and through Clark v. Snap, Inc., No. 21-cv-9, 2021 WL 2376359, at*3 (S.D. Ill. June 10, 2021).

219 *See, e.g.*, Jacobowitz v. Experian Info. Sols., Inc., Civ. No. 19-20120, 2021 WL 651160, at *4–5 (D.N.J. Feb. 19, 2021).

Privacy scholars have recognized the threat that the Court's FAA jurisprudence poses for privacy law. As Lindsey Barrett succinctly puts it: "[A] private right of action in federal privacy legislation that isn't accompanied by a ban on forced arbitration for applicable rights will be absolutely useless."[220] Others have echoed the point.[221]

In sum, the Federal Arbitration Act is a significant impediment to the efficacy of a private right of action. Absent an arbitration carveout, a privately enforceable privacy law will inevitably prove futile thanks to expansive preemption and an empty effective-vindication rule.

A second and distinct manifestation of the problem with adhesion contracts is unique to privacy law. Terms of service don't just compel individualized arbitration; they "also attempt to require users . . . to give broad prospective consent to information collection and use, thereby effectively disclaiming any argument that mass data harvesting constitutes injury in the first place."[222] In other words, arbitration clauses are a procedural obstacle—users can still theoretically pursue their claims in the arbitral forum, though we've just seen that the practical reality is they can't and won't. Consent, on the other hand, operates as a substantive obstacle—defeating a privacy law claim on the merits.

Technology companies have pressed the point explicitly. In litigation arising from the Cambridge Analytica scandal, Facebook's counsel contended at oral argument: "Once you have that consent, which is plain and clear and we believe as a matter of law enforceable against the plaintiffs, a person cannot be injured in fact by the sharing of information when the person consented to that very sharing of information."[223] And of course the "consent" to which he's referring is an opaque disclosure squirreled away deep inside a thicket of legal jargon deliberately drafted to avoid actually being read or understood.[224]

220 Lindsey Barrett (@LAM_Barrett), TWITTER (Sept. 20, 2019, 8:51 AM), https://twitter.com/LAM_Barrett/status/1175029614684581889 [https://perma.cc/VCE9-HCUQ].

221 *See, e.g.*, Daniel Wilf-Townsend, *The Fine Print That Could Undermine New Internet Privacy Legislation*, WASH. POST (Mar. 11, 2019, 6:00 AM), www.washingtonpost.com/outlook/2019/03/11/fine-print-that-could-undermine-new-internet-privacy-legislation/ [https://perma.cc/H37J-NBNE]; 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/X4LG-GYMJ].

222 Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 557 (2017).

223 Transcript of Oral Argument at 8, *In re* Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767 (N.D. Cal. 2019) (No. 18–md–2843).

224 For the specifics of the relevant Facebook terms of service, see *In re Facebook*, 402 F. Supp. 3d at 789–92. For the proposition that terms of service are not actually read and are intended not to be read, see, for example, Michael Karanicolas, *Too Long; Didn't Read: Finding Meaning in Platforms' Terms of Service Agreements*, 52 U. TOL. L. REV. 1, 3 & nn.6–8 (2021).

While the district court refused to accept that particular consent argument at the motion-to-dismiss stage,[225] other businesses have successfully used boilerplate consent to defeat privacy claims later in litigation.[226]

Many scholars have focused on the crucial role that consent plays in privacy and data protection law. Scholars have persuasively shown that consent—often called "notice and choice" or, more accurately, "notice and waiver"—is a poor mechanism for promoting and protecting privacy.[227] Unfortunately, few policymakers are attuned to these critiques. Julie Cohen summed up a survey of federal privacy law proposals by saying, "[t]he continuing optimism about consent-based approaches to privacy governance is mystifying, because the deficiencies of such approaches are well known and relatively intractable."[228]

Fewer scholars have explored the specific question of notice-and-waiver's effects on private rights of action within privacy law.[229] Cohen has argued, "[v]irtual agreements defining a broad range of permitted information practices and a narrow and possibly nonexistent range of permitted remedies sketch an information environment characterized by starkly uneven distributions of power."[230] She contends that by "validating those agreements, consent-based dismissals of information privacy claims constitute a powerful statement of institutional disengagement from the conditions of contemporary commercial life."[231]

In sum, courts' widespread enforcement of adhesion contracts is a significant obstacle to a privacy private right of action. Not only will privacy plaintiffs be bound to individualized arbitration, terms of service can also easily defeat their claims on the merits.

2. Standing

Even if a plaintiff can keep her privacy claim in federal court, she faces a second significant hurdle: the intangibility of privacy harms.

---

225 *See In re Facebook*, 402 F. Supp. 3d at 787–95.

226 *See, e.g.*, Ginwright v. Exeter Fin. Corp., 280 F. Supp. 3d 674, 681–90 (D. Md. 2017) (declining to certify a TCPA class on consent grounds).

227 *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–83 (2013); Julie E. Cohen, *Turning Privacy Inside out*, 20 THEORETICAL INQUIRIES L. 1, 6, 20 (2019); *see also infra* subsection III.B.1.

228 COHEN, *supra* note 12, at 4.

229 *Cf.* Waldman, *supra* note 15 (manuscript at 36–40); Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 310, 314–15 (2019).

230 Cohen, *supra* note 222, at 561.

231 *Id.*

Article III of the U.S. Constitution provides that the federal judicial power extends to cases and controversies.[232] In recent decades, the Supreme Court has interpreted this simple provision to limit who can maintain a lawsuit in federal court and to what kinds of claims federal jurisdiction extends. This doctrine is called Article III standing, and it requires that plaintiffs show an injury in fact, causation, and redressability.[233] The Court has further defined the injury in fact criterion to mean a concrete and particularized injury that is actual or imminent and not speculative or conjectural.[234]

While now routine, the Court only began invalidating legislation that authorized private plaintiffs' suits in the past 30 years.[235] The Court's initial justification for doing so was premised on preventing judicial interference with the executive branch.[236] But in the past decade, the Court has repeatedly gone further—invalidating congressionally authorized private rights of action in suits against private-sector defendants, reasoning that some intangible injuries are insufficiently "concrete."[237] This doctrinal development has culminated most recently in a 2021 Supreme Court decision that has foreboding implications for privacy laws—both enacted and proposed—that employ a private right of action.

TransUnion is one of the three major credit-reporting companies in the United States.[238] For over a decade, TransUnion cross-referenced credit-check subjects' first and last names against the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC") list.[239] The OFAC list includes suspected terrorists and other serious criminals, and federal law prohibits transacting with people on the OFAC list.[240] Using only first and last names produced thousands upon thousands of false positives, including Sergio Ramirez.[241] Ramirez was denied credit when TransUnion attached an erroneous OFAC designation to his credit report, and he filed a class action against

232 U.S. CONST. art. III, §§ 1–2.

233 *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) (citing Allen v. Wright, 468 U.S. 737, 756 (1984)).

234 *See id.* at 560.

235 *See* Peter C. Ormerod, *Privacy Injuries and Article III Concreteness*, 48 FLA. ST. U. L. REV. 133, 139–41 (2021); *see also id.* at 136 nn.6–17 (listing Article III cases during the Roberts Court).

236 *See* Peter Ormerod, *Making Privacy Injuries Concrete*, 79 WASH. & LEE L. REV. 101, 127–30 (2022)

237 *See id.* at 119–24.

238 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021).

239 *Id.*; *see id.* at 2215 (Thomas, J., dissenting).

240 *Id.* at 2201 (majority opinion).

241 *See id.* at 2201–02; *id.* at 2215–16 (Thomas, J., dissenting) (summarizing Cortez v. Trans Union, LLC, 617 F.3d 688 (3d Cir. 2010)).

TransUnion, alleging multiple violations of the FCRA.[242] The district court certified a class that included 8,185 people whom TransUnion also falsely designated an OFAC match during a seven-month period, and the parties stipulated that TransUnion had proof that 1,853 of those class members actually had the false designation disseminated to a potential creditor, employer, or landlord.[243] Ramirez won at trial and the Ninth Circuit affirmed in relevant part.[244]

In a 5–4 decision, the Supreme Court vacated and remanded.[245] The Court first held that only the 1,853 people who could show actual third-party dissemination had a sufficiently concrete injury for Article III purposes; the other 6,332 did not.[246] The Court analyzed Ramirez's claim by looking to historical practice and determined that only those plaintiffs who could show actual dissemination had suffered an injury that was sufficiently analogous to common-law defamation.[247] As for those who couldn't show third-party dissemination, the Court explained that the "mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."[248]

The Court also concluded that only Ramirez had a sufficiently concrete injury to pursue FCRA violations arising from the inaccurate and confusing mailings the company sent to class members when they requested their own credit reports.[249] The plaintiffs, the Court held, "presented no evidence that, other than Ramirez, a single other class member so much as opened the dual mailings, nor that they were confused, distressed, or relied on the information in any way."[250] Because the absent class members had failed to supply "any evidence of harm caused by the format of the mailings," these injuries were "bare procedural violations, divorced from any concrete harm."[251]

The majority also brushed back two alternative theories the plaintiffs advanced. First, the Court held that the 6,332 plaintiffs that were unable to prove actual dissemination could not rely on an increased risk of injury as a basis for standing.[252] The Court seems to hold that

242 *TransUnion*, 141 S. Ct. at 2201–02.

243 *Id.* at 2202.

244 *Id.*

245 *Id.* at 2200.

246 *See id.* at 2208–13.

247 *See id.* at 2209–10.

248 *Id.* at 2210.

249 *See id.* at 2213–14.

250 *See id.* at 2213 (quoting Ramirez v. TransUnion LLC, 951 F.3d 1008, 1039, 1041 (9th Cir. 2020) (McKeown, J., concurring in part and dissenting in part) (internal quotation marks and emphasis omitted)).

251 *Id.* (internal quotation marks and alterations omitted) (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)).

252 *See id.* at 2209–13.

increased future risk claims are never sufficient for Article III when a plaintiff seeks damages.[253] Instead, increased risk claims are only actionable when a plaintiff seeks injunctive relief.[254]

Second, the 6,332 plaintiffs that were unable to prove actual dissemination also argued that the emotional anguish associated with receiving a false OFAC designation was sufficiently analogous to intentional infliction of emotional distress.[255] In an opaque footnote, the Court took "no position on whether or how such an emotional or psychological harm could suffice for Article III purposes," but nevertheless also concluded that the argument was unpersuasive because "the 6,332 plaintiffs have not established that they were even aware of the misleading information in the internal credit files maintained at TransUnion."[256]

TransUnion and its ilk are an enormous problem for enacted and proposed privacy laws that rely on a private right of action to bolster enforcement and incentivize compliance.

Start with the Court's historical analysis. As many scholars and judges have explained, the historical basis for Article III standing doctrine is dubious.[257] Given this murky history, it's unclear why the concreteness analysis requires a "close relationship" between new and old private rights of action. William Baude has argued that, with privacy law, it "is unclear why . . . Congress should not be allowed to protect interests beyond those protected by the common law, as it has been allowed in other cases."[258]

And privacy law is a realm in dire need of space for innovation and flexibility in defining legal rights, duties, and harms. According to *TransUnion*, policymakers confront a world of novel harms arising from digitally enabled networked information technologies armed only with analogies to the four privacy torts William Prosser fashioned in 1960.[259] It's difficult to see, for example, how reliance on intrusion upon seclusion can possibly be responsive to claims involving facial

253 *See id.*

254 *See id.* at 2210–11.

255 *See id.* at 2211 n.7.

256 *See id.*

257 *See, e.g.*, Cass R. Sunstein, *What's Standing After* Lujan*? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 166 (1992); John A. Ferejohn & Larry D. Kramer, *Independent Judges, Dependent Judiciary: Institutionalizing Judicial Restraint*, 77 N.Y.U. L. REV. 962, 1009 (2002); *TransUnion*, 141 S. Ct. at 2216–21 (Thomas, J., dissenting).

258 William Baude, *Standing in the Shadow of Congress*, 2016 SUP. CT. REV. 197, 223; *see also* Ormerod, *supra* note 236, at 131–36 (arguing that the separation of powers cannot justify *TransUnion*'s reasoning).

259 *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); *see, e.g.*, Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462–63 (7th Cir. 2020) (analogizing a TCPA violation to intrusion upon seclusion).

recognition harms or targeted advertising's metastasized surveillance infrastructure.[260] Daniel Solove and Danielle Keats Citron have highlighted this incoherency, noting that Prosser's torts weren't widely recognized until after he helped codify them in the Restatement (Second) of Torts.[261]

The Court's analysis of the risk of future harm is similarly troubling. Several privacy scholars have persuasively argued that the issue of increased risk is one of the most fundamental shifts enabled by technological change.[262] Legislatures are now unable to employ statutory damages unless a plaintiff can identify a past or present injury that certainly materialized.[263]

One rejoinder to difficult questions about risk is to turn inward and recognize subjective harms associated with abusive informational practices.[264] Yet *TransUnion* is an impediment here too. The Court rejects the intuitive notion that requesting and receiving a credit report that falsely labels you a terrorist bears a close relationship to the extreme and outrageous conduct actionable at common law.[265] The Court concedes that Ramirez was sufficiently distressed and confused by the mailings to confer a concrete injury, but that absent class members had simply failed to offer adequate proof of a similar experience.[266] The particular way the Court ducks this issue—by demanding individualized proof from absent class members—is highly impractical in most privacy law litigation because low-dollar statutory damage awards are only feasible to pursue in a class posture and demanding individualized proof from thousands of absent class members is a self-defeating proposition.[267]

Both before and after *TransUnion*, lower courts have dismissed privacy class actions by relying on the Court's standing decisions.[268] For example, both the Seventh and Eighth Circuits have held that

260 *See, e.g.*, Ormerod, *supra* note 235, at 180–83.

261 *See* Solove & Citron, *supra* note 195, at 67.

262 *See, e.g.*, COHEN, *supra* note 74, at 149–51; Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756–61 (2018).

263 Data breaches provide a particularly stark illustration of this problem. *Cf.* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021) (setting forth three nonexhaustive factors for evaluating Article III standing in data breach cases, all of which allow for increased risk of future harm).

264 *See, e.g.*, Solove & Citron, *supra* note 262, at 764–74; M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1144–47 (2011).

265 *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2211 n.7 (2021).

266 *See id.* at 2208–09, 2011.

267 *See infra* subsection II.B.3.

268 *See, e.g.*, Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 929–31 (8th Cir. 2016); Verde v. Confi-Chek, Inc., No. 21-C-50092, 2021 WL 4264674, at *5 (N.D. Ill. Sept. 20, 2021).

retaining customer data in violation of the Cable Communications Policy Act does not constitute a concrete injury.[269]

Privacy scholars in recent years have identified the stark problems with the Court's standing doctrine and have offered proposals for resolving its incoherencies. Danielle Citron and Daniel Solove have sought to taxonomize privacy harms and connect these harms to the concrete injury inquiry.[270] Jonathon W. Penney has argued that courts should recognize that social conformity is a concrete Article III injury in fact.[271] Ignacio Cofone has offered a three-step framework for identifying actionable privacy harms.[272] And in past work, I have argued that if courts refuse to defer to the legislature when confronting informational injuries, privacy theory can help offer a solution for distinguishing between sufficiently and insufficiently concrete injuries.[273]

Despite these developments, the federal courts—led by the Supreme Court—continue their inexorable campaign to eliminate jurisdiction over a vast array of surveillance harms. Given the constitutional footing of standing doctrine, policymakers need tools other than the private right of action to ensure rigorous enforcement of privacy law.

3. Class Certification

The final shortcoming with a private right of action is its inevitable reliance on class actions. We have seen how the shortcomings discussed above inevitably implicate class actions: compelled arbitration forces plaintiffs to adjudicate their claims individually,[274] and Article III standing forces plaintiffs to include detailed individualized allegations that make class certification difficult.[275] The shortcoming discussed here focuses on a final piece of the impracticalities of privacy law private rights of action: the courts' interpretations of Federal Rule of Civil Procedure 23.

---

269 *See Braitberg*, 836 F.3d at 929–31; Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 911–13 (7th Cir. 2017).

270 *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 831 (2022); Solove & Citron, *supra* note 262, at 785–86; Solove & Citron, *supra* note 195, at 69.

271 *See* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1488–1530 (2022).

272 *See* Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367, 1369.

273 *See* Ormerod, *supra* note 235, at 168–72 (arguing for a deference approach); Ormerod, *supra* note 236, at 153–75 (proposing a framework based on contextual integrity).

274 *See, e.g.*, *supra* notes 213–15.

275 *See, e.g.*, Cordoba v. DirecTV, LLC, 942 F.3d 1259, 1272–77 (11th Cir. 2019); Richard M. Re, *Talking About Standing in Zivotofsky and Robins*, PRAWFSBLAWG (May 17, 2015), https://prawfsblawg.blogs.com/prawfsblawg/2015/05/talking-about-standing-in-zivotofsky-and-spokeo.html [https://perma.cc/888Q-LXBF] (discussing the tension between pleading sufficient facts to establish standing and pleading too many facts to certify a class).

Rule 23(a)(2) requires that there be "questions of law or fact common to the class."[276] Like the other Rule 23(a) factors, establishing commonality is necessary to certify any type of class action. The plain text of Rule 23(a)(2) would seem to establish an easy-to-clear hurdle, "since '[a]ny competently crafted class complaint literally raises common "questions."'"[277]

And yet the Court disregarded that plain language and heightened the commonality criterion in *Wal-Mart Stores, Inc. v. Dukes*.[278] The Court held that commonality requires that every class member must suffer the "same injury."[279] The same injury, however, "does not mean merely that they have all suffered a violation of the same provision of law."[280] Instead, the class's "claims must depend upon a common contention," and that common contention "must be . . . capable of classwide resolution—which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke."[281]

The *Wal-Mart* dissent argued that the majority had conflated commonality with Rule 23(b)(3)'s requirement that "questions of law or fact common to class members predominate over any questions affecting only individual members."[282] Unlike commonality, the predominance inquiry is not a prerequisite to certifying all classes; instead, the "more demanding" predominance requirement only applies to classes that seek damages.[283]

Two years later, the same *Wal-Mart* majority turned its attention to predominance. In *Comcast Corporation v. Behrend*, a consumer antitrust class action, the Court held that the proposed class failed the predominance inquiry because its statistical model for measuring damages failed to identify the precise damages attributable to the particular antitrust injury alleged.[284]

The grant and opinion in *Comcast* were peculiar due to how factbound the issue was.[285] But scholars have argued that *Wal-Mart* and

276 FED. R. CIV. P. 23(a)(2).

277 Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 349 (2011) (quoting Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97, 131–32 (2009)) (alteration original).

278 *See id.*at 350.

279 *See id.* at 349–50 (quoting General Tele. Co. v. Falcon, 457 U.S. 147, 157 (1982)).

280 *Id.* at 350.

281 *Id.*

282 FED. R. CIV. P. 23(b)(3); *see Wal-Mart*, 564 U.S. at 375–77 (Ginsburg, J., concurring in part and dissenting in part).

283 *See Wal-Mart*, 564 U.S. at 367–68, 375 (Ginsburg, J., concurring in part and dissenting in part).

284 Comcast Corp. v. Behrend, 569 U.S. 27, 34–38 (2013).

285 *See id.* at 38–43 (Ginsburg & Breyer, JJ., dissenting).

Comcast are part of a marked shift in the Court's class action jurisprudence—from requiring common questions to requiring common answers.[286] And there can be little doubt there is a trend of general antagonism towards class actions at the Supreme Court. In addition to defendant victories in *Wal-Mart*, *Comcast*, and *TransUnion*, the Court ruled against class action plaintiffs in 2016's *Spokeo, Inc. v. Robins*,[287] 2019's *Frank v. Gaos*,[288] and 2020's *Thole v. U.S. Bank N.A.*.[289]

Class action skepticism is not, however, limited to the Supreme Court. The lower federal courts are also finding atextual reasons for refusing to certify classes. For example, several federal circuits have imposed an "ascertainability" requirement for damages classes under Rule 23(b)(3). The ascertainability criterion provides that if "class members are impossible to identify without extensive and individualized fact-finding or 'mini-trials,' then a class action is inappropriate."[290] Ascertainability is the subject of a deep and widening circuit split,[291] so a future Supreme Court decision that endorses a stringent ascertainability requirement would hardly be surprising.

These developments have foreboding implications for privacy law litigation. Lower courts have repeatedly declined to certify privacy class actions by relying on the ever-heightening commonality, predominance, and ascertainability requirements. For example, in litigation that alleged Facebook's scanning of the contents of users' direct messages violated federal and California wiretapping prohibitions, the district court refused to certify a damages class under Rule 23(b)(3).[292] Even though both laws provide for statutory damages, the district court concluded that "many class members appear to have suffered little, if any, harm."[293] The lack of harm, the court concluded, meant that "many individual damages awards would be disproportionate, and

286 *See, e.g.*, A. Benjamin Spencer, *Class Actions, Heightened Commonality, and Declining Access to Justice*, 93 B.U. L. REV. 441, 444 (2013); Daniel Jacobs, Comment, Comcast Corp. v. Behrend*: Common Questions Versus Individual Answers—Which Will Predominate?*, 47 LOY. L.A. L. REV. 505, 506 (2014).

287 Spokeo, Inc. v. Robins, 578 U.S. 330, 342–43 (2016).

288 Frank v. Gaos, 139 S. Ct. 1041, 1043–44 (2019) (per curiam).

289 Thole v. U.S. Bank N.A., 140 S. Ct. 1615, 1619 (2020).

290 Marcus v. BMW of North America, LLC, 687 F.3d 583, 592–94 (3d Cir. 2012).

291 *See, e.g.*, *id.*; Mullins v. Direct Digit., LLC, 795 F.3d 654, 657–58 (7th Cir. 2015) ("Nothing in Rule 23 mentions or implies this heightened requirement under Rule 23(b)(3), which has the effect of skewing the balance that district courts must strike when deciding whether to certify classes."); Cherry v. Dometic Corp., 986 F.3d 1296, 1301–03 (11th Cir. 2021). *See generally* Rhonda Wasserman, *Ascertainability: Prose, Policy, and Process*, 50 CONN. L. REV. 695 (2018).

292 *See* Campbell v. Facebook Inc., 315 F.R.D. 250, 264–69 (N.D. Cal. 2016).

293 *Id.* at 269.

sorting out those disproportionate damages awards would require individualized analyses that would predominate over common ones."[294]

As for ascertainability, in litigation that alleged Hulu violated the Video Privacy Protection Act by disclosing personal information to unauthorized third parties, the district court also refused to certify a damages class.[295] The court determined that—due to the complexity of the company's technical protocols—the only way to identify class members was by asking: "do you log into Facebook and Hulu from the same browser; do you log out of Facebook; do you set browser settings to clear cookies; and do you use software to block cookies?"[296] Because the law's statutory damages awards are relatively high and because of the "vagaries of subjective recollection," the court concluded that the class wasn't ascertainable.[297]

The scholars and commentators who have waded into the privacy class action quagmire have had few charitable things to say about these and similar decisions. Nathan Webster has noted that "privacy class actions, with their vast scope and technical sophistication, are particularly vulnerable to arbitrary judicial determinations of ascertainability and 'manageability' that lead to conflicting, unpredictable results for different suits."[298] Webster sums up the current landscape by arguing that "courts are making capricious ascertainability determinations and, in doing so, are perseverating on policy considerations that uniquely penalize data privacy class actions for indolent recordkeeping by defendants."[299] Ultimately, these decisions suggest that "in information privacy litigation, no class claims may be maintained for monetary relief of any sort, even when the wrongdoing consists of market-wide conduct for which Congress has provided a uniform remedy."[300]

* * *

It's useful, at this point, to consider how the doctrines discussed in this Section fit together. Imagine that Congress does enact a privacy

294 *Id.*

295 *See In re:* Hulu Priv. Litig., No. C 11–03764, 2014 WL 2758598, at *1 (N.D. Cal. June 17, 2014).

296 *Id.* at *16; *see also id.* at *14 ("[C]lass members are those who actually had their [personally identifiable information] transmitted to Facebook. That inquiry turns on whether the c_user cookie was sent to Facebook, which depends on a number of variables (including whether the user remained logged into Facebook, cleared cookies, or used ad-blocking software).").

297 *See id.* at *16; *see also* 18 U.S.C. § 2710(c)(2)(A) (2018).

298 Nathan Webster, Note, *Whose Data Anyway? The Inconsistent and Prejudicial Application of Ascertainability in Data Privacy Class Actions*, 105 MINN. L. REV. 2551, 2568 (2021).

299 *Id.* at 2554, 2568–80.

300 Cohen, *supra* note 222, at 566.

statute that has a private right of action, that it provides for statutory damages, but that it does not include an FAA carveout.

Putative class action plaintiffs face an uphill battle to hold companies accountable for violating the statute. First, plaintiffs will need to avoid terms of service that seek blanket consent for the informational practices that violate the statute—something over which the plaintiffs have no control. Second, the plaintiffs will also need to avoid individualized arbitration clauses in those same terms of service—which they also cannot influence. Third, the federal courts will lack jurisdiction over the dispute unless the plaintiffs convince the court that their statutory claims face a sufficiently "close relationship" to one of Prosser's four privacy torts. And even if they make it past the motion-to-dismiss stage, the plaintiffs will also have to run the gamut of commonality, predominance, and ascertainability to have their class certified. Failure on any of these half-dozen requirements will render the action infeasible or impossible to pursue, at least in federal court.[301]

Given this avalanche of difficulties, policymakers need tools other than the private right of action to ensure that privacy laws will be rigorously and effectively enforced. The next Part proposes one such possibility.

III. QUI TAM ENFORCEMENT

So far, we've seen that public enforcement is often ineffective and private enforcement is often impossible. To find a solution to this enforcement vice, this Part surveys and proposes a hybrid approach: qui tam enforcement.

A. Examples

A qui tam is "an action under a statute that allows a private person to sue for a penalty, part of which the government or some specified public institution will receive."[302] The term itself is Latin for "who as well," as in the "plaintiff is a suitor 'who as well' sues for the state."[303] This Section surveys qui tam's origins and then turns to the False

301 The state court question is more complex and variable. About half the states follow some version of the Supreme Court's constitutional standing doctrine. *See* Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC., & NAT. RES. L. 349, 349, 353 (2015). Most—though not all—states have class actions, but state-law rules of procedure vary widely. *See generally* AM. BAR ASS'N, CLASS ACTIONS & DERIVATIVE SUITS COMM., THE LAW OF CLASS ACTION: FIFTY-STATE SURVEY (2020). And the arbitration issue is particularly acute for state law claims. *See, e.g.*, AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 341 (2011); *supra* notes 206–08.

302 BRYAN A. GARNER, GARNER'S DICTIONARY OF LEGAL USAGE 745 (3d ed. 2011).

303 *Id.*

Claims Act—federal law's most prominent qui tam enforcement scheme.

1. Older Qui Tam

Qui tam actions have an ancient pedigree. They originated as a common-law action in England in the thirteenth century, and Parliament enacted several in statute in the fifteenth century.[304]

In the United States, qui tam suits have "been in existence . . . ever since the foundation of our Government."[305] In the seventeenth century, American colonists enacted qui tam statutes, and colonial courts heard qui tam cases arising under both colonial and English law.[306] Colonial qui tam statutes, for example, authorized relators to receive half the damages recovered for pursuing people who fished for mackerel and oysters out of season and who peddled without a license.[307]

Following the Framing, the First Congress enacted statutes that authorized qui tam enforcement for failing to return census reports, harboring runaway sailors, trading with Native American tribes without a license, and failing to pay customs.[308] The early federal courts adjudicated qui tam disputes, but by "the turn of the twentieth century, qui tam statutes had largely fallen into disuse in this country, although they often remained on the books."[309]

Today, there "is no common-law right to bring a *qui tam* action, which is strictly a creature of statute."[310] The qui tam label encompasses several distinct but related types of actions, and the False Claims Act (FCA) is the most prominent example of a federal law that

304 *Id.*; *see also* Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 774–76 (2000).

305 Marvin v. Trout, 199 U.S. 212, 225 (1905).

306 *See* CHARLES DOYLE, CONG. RSCH. SERV., R40785, QUI TAM: THE FALSE CLAIMS ACT AND RELATED FEDERAL STATUTES 3–4 (2021).

307 *See id.* at 3 n.19 (citing CITY OF BOSTON, THE COLONIAL LAWS OF MASSACHUSETTS: REPRINTED FROM THE EDITION OF 1672, WITH THE SUPPLEMENTS THROUGH 1686, at 54 (Boston, Rockwell & Churchill 1887) (1672) (penalties for catching mackerel out of season to be distributed one half to the informer and one half to the town where the offense occurred); 1 CHARLES Z. LINCOLN, WILLIAM H. JOHNSON & A. JUDD NORTHRUP, THE COLONIAL LAWS OF NEW YORK FROM THE YEAR 1664 TO THE REVOLUTION 845 (Albany, James B. Lyon 1894) (twenty-shilling penalties for taking oysters out of season to be distributed half to the informer and half to the benefit of the poor of the town where the offense occurred); 2 LINCOLN ET AL., *supra*, at 989–90 (penalties of £30 for peddling without a license to be distributed one moiety to the informer and one for the benefit of the town where the offense occurred).

308 *See id.* at 4 n.22 (citing these examples); *see also Stevens*, 529 U.S. at 776–77, nn.5–7 (citing additional examples).

309 DOYLE, *supra* note 306, at 4.

310 United Seniors Ass'n, Inc. v. Philip Morris USA, 500 F.3d 19, 23 (1st Cir. 2007).

authorizes qui tam enforcement.[311] The FCA was originally enacted in 1863, and it imposes civil liability upon "any person who . . . knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval" to an officer or employee of the United States government.[312] The defendant is liable for a civil penalty of up to $10,000 plus three "times the amount of damages which the Government sustains because of the act of that person."[313] There are two ways to commence an FCA action: First, the government may bring a civil action against the alleged false claimant.[314] Second, a private person called a relator may bring a qui tam civil action "for the person and for the United States Government" against the alleged false claimant "in the name of the Government."[315]

If a relator seeks to initiate an FCA action, she must first deliver a copy of the complaint with any supporting evidence to the government.[316] The government has sixty days to decide whether to intervene.[317] If the government decides to intervene, it assumes the primary responsibility prosecuting the action,[318] but the relator retains three rights: to continue as a party to the action, to a hearing before voluntary dismissal, and to a court determination of reasonableness before settlement.[319] If the government declines to intervene, the relator has the exclusive right to prosecute the action,[320] and the government may intervene thereafter only on a showing of good cause.[321] Whether or not the government intervenes, the relator is entitled to a share of any proceeds recovered. If the government intervenes, the relator is entitled to between fifteen and twenty-five percent; if not, the relator is entitled to between twenty-five and thirty percent, plus attorney's fees and costs.[322]

---

311 *See* DOYLE, *supra* note 306, at 1–4.

312 Act of March 2, 1863, ch. 67, §§ 1–9, 12 Stat. 696, 696–99 (codified at 31 U.S.C. § 3729(a)(1) (2018)).

313 31 U.S.C. § 3729(a)(1)(G) (2018).

314 *Id.* § 3730(a).

315 *Id.* § 3730(b)(1).

316 *See id.* § 3730(b)(2).

317 *See id.*; *id.* § 3730(b)(4).

318 *Id.* § 3730(c)(1).

319 *Id.* § 3730(c)(1)–(2)(B).

320 *Id.* § 3730(b)(4)(B).

321 *Id.* § 3730(c)(3). Federal circuit courts have sharply divided over the government's authority to dismiss FCA suits that government initially declined to prosecute. *Compare* United States *ex rel.* Sequoia Orange Co. v. Baird-Neece Packing Corp., 151 F.3d 1139, 1143 (9th Cir. 1998), *with* Swift v. United States, 318 F.3d 250, 251 (D.C. Cir. 2003). The Supreme Court is poised to soon resolve the conflict. *See* United States *ex rel.* Polansky v. Exec. Health Res., Inc., 142 S. Ct. 2834 (2022).

322 *See* 31 U.S.C. § 3730(d)(1)–(2) (2018).

The Supreme Court addressed whether an FCA relator has Article III standing in 2000's *Vermont Agency of Natural Resources v. United States ex rel. Stevens*. Stevens was a former employee of the Vermont Agency of Natural Resources, and he filed a qui tam suit against his former employer, alleging that it had submitted claims to the Environmental Protection Agency that overstated the amount of time spent by its employees on federally funded projects.[323] The government declined to intervene, and the Supreme Court addressed two questions—whether Stevens had Article III standing to maintain the suit and whether the state of Vermont (or an agency thereof) was a "person" subject to liability under the FCA.[324] The Court concluded that Stevens did have Article III standing but that the statute did not authorize suits against states.[325]

The majority's standing discussion provides critical insight about the constitutionality of any qui tam proposal. The Court distinguished between two types of qui tam models—agency and assignment. On the agency model, the relator simply stands in the shoes of the government; the relator is the government's agent and asserts only the government's interest on behalf of the government.[326] On the assignment model, the statute assigns (or partially assigns) to the relator the government's damages claim.[327]

The Court explained that, on the agency model, the relator automatically satisfies the strictures of Article III. It would suffice for Article III standing, the Court explained, if the relator was "simply the statutorily designated agent of the United States, *in whose name* . . . the suit is brought—and that the relator's bounty is simply the fee he receives *out of the United States' recovery* for filing and/or prosecuting a successful action on behalf of the Government."[328] But, the Court held, the FCA didn't employ the agency model because the FCA "gives the relator himself an interest *in the lawsuit*, and not merely the right to retain a fee out of the recovery."[329] Instead, the Court concluded, the FCA "can reasonably be regarded as effecting a partial assignment of the Government's damages claim."[330] Because the United States suffered an injury in fact—in the form of an injury to its property—the FCA partially

323 *See* Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 770–71 (2000).

324 *See id.*

325 *See id.* at 771–78 (standing); *id.* at 778–87 (statutory interpretation).

326 *See* Gilles & Friedman, *supra* note 41, at 521.

327 *See id.* at 522.

328 *See Stevens*, 529 U.S. at 772.

329 *Id.*

330 *Id.* at 773.

assigned the government's claim to the relator, and "the United States' injury in fact suffices to confer standing on respondent Stevens."[331]

Myriam Gilles and Gary Friedman have helpfully expounded upon the distinction between the agency and assignment models. On the agency model, Article III standing "is predicated on the government's general enforcement powers, and not on any injury-in-fact the government happens to have suffered in its proprietary capacity."[332] On the other hand, "in cases where the government has suffered injury to its property, relator standing might be grounded in a theory of assignment, where the government partly assigns its claim—and its injury-in-fact, as the aggrieved party—to the relator."[333] The agency model was inappropriate in *Stevens*, Gilles and Friedman explain, "because the FCA expressly provides that the relator remains a party, even where the Government takes the case over, and the relator may challenge any settlement or dismissal of the action."[334] The distinction between agency and assignment may seem rather fine, but Gilles and Friedman have shown that the distinction can prove incredibly consequential in practice.[335]

Scholars have studied the FCA far beyond the narrow question of Article III standing. Some have considered the FCA's separation-of-powers implications,[336] while others have used the FCA to launch broader investigations of the American legal system's unique enforcement pathologies.[337] David Freeman Engstrom, for example, has exhaustively documented the on-the-ground realities of FCA litigation.[338] Among other insights, Engstrom has found little evidence to support critics' refrains about the FCA and qui tam enforcement more generally—that there has been an inefficient explosion in FCA litigation in recent decades,[339] that FCA litigation is dominated by a small number of "professional" plaintiff–relators,[340] and that an increasingly

331 *Id.* at 774.

332 Gilles & Friedman, *supra* note 41, at 521–22.

333 *Id.* at 522.

334 *Id.*

335 *See id.* at 528–31.

336 *See infra* subsection III.D.3.

337 *See, e.g.*, David Freeman Engstrom, *Jacobins at Justice: The (Failed) Class Action Revolution of 1978 and the Puzzle of American Procedural Political Economy*, 165 U. PA. L. REV. 1531, 1534 (2017).

338 *See, e.g.*, David Freeman Engstrom, *Harnessing the Private Attorney General: Evidence from Qui Tam Litigation*, 112 COLUM. L. REV. 1244, 1249 (2012) [hereinafter Engstrom, *Harnessing*]; David Freeman Engstrom, *Public Regulation of Private Enforcement: Empirical Analysis of DOJ Oversight of Qui Tam Litigation Under the False Claims Act*, 107 NW. U. L. REV. 1689, 1689 (2013); David Freeman Engstrom, *Private Enforcement's Pathways: Lessons from Qui Tam Litigation*, 114 COLUM. L. REV. 1913, 1921 (2014) [hereinafter Engstrom, *Pathways*].

339 *See* Engstrom, *Pathways*, *supra* note 338, at 1951–63.

340 *See* Engstrom, *Harnessing*, *supra* note 338, at 1275–81, 1288–98.

specialized qui tam plaintiffs' bar is responsible for perceived excesses of FCA litigation.[341] At the same time, however, Engstrom has suggested that the government's gatekeeping authority over FCA claims may offer some notable advantages over both purely public and purely private enforcement schemes. Because "[p]rivate enforcers will progressively target regulatory ambiguities left by legislative or administrative inertia," private enforcement has a tendency to "push legal mandates down interpretive pathways they would not travel with purely public enforcement."[342] Qui tam's gatekeeping authority enables resourced-constrained and risk-averse agencies "to rely upon private enforcers to test the waters in federal court before diving in and spending the agency's reputational capital and resources."[343]

2. Newer Qui Tam

After *Stevens*, the most prominent example of a new statute with a qui-tam-like enforcement mechanism is California's Private Attorneys General Act (PAGA).[344] Enacted in 2004, PAGA authorizes an "aggrieved employee" to bring suit "on behalf of himself or herself and other current or former employees" to recover penalties for violations of the Labor Code.[345] The law defines an "aggrieved employee" as an employee "against whom one or more of the alleged violations was committed."[346]

The state's justification for enacting the law was that severe understaffing of public enforcement agencies allowed employers to "violate the law with impunity."[347] California employment lawyers say that "PAGA has markedly improved employer compliance with statutory and regulatory mandates over the past decade," and the law supplies the state treasury with about $4 million per year in revenue.[348]

More recently, Gilles and Friedman have urged the adoption of what they call the "new qui tam": state laws that use qui tam actions to fill the enforcement gap left by disinterested and underfunded public regulators and by doctrinal impediment to private rights of action.[349]

---

341 *See id.* at 1281–85, 1298–1306.

342 *See* Engstrom, *Pathways*, *supra* note 338, at 1968.

343 *Id.* at 1986–87.

344 CAL. LAB. CODE §§ 2698–2699.8 (West 2022).

345 *Id.* § 2699(a).

346 *Id.* § 2699(c).

347 *See* Gilles & Friedman, *supra* note 41, at 494 (quoting ASSEMB. COMM. ON JUDICIARY, COMM. ANALYSIS OF S.B. 796, S. 2003-796, 1st Extraordinary Sess., at 3–4 (Cal. 2003)).

348 *Id.* at 494–95 (citing Laura Reathaford & Eric Kingsley, *He Said, She Said: Employment Litigators Debate California's Private Attorneys General Act*, WESTLAW J. EMP., June 7, 2016, at 1; *id.* at 495 n.25 (citing CAL. DEP'T OF INDUS. RELS., BUDGET CHANGE PROPOSAL 1 (2016)).

349 *Id.* at 491, 494.

The new qui tam, Gilles and Friedman argue, is essential for protecting group rights and furthering important social policies in an otherwise hostile environment.[350] In addition to protecting workers, Gilles and Friedman observe that "[a]nother area that is ripe for qui tam is consumer protection—a field left especially vulnerable by federal agency inaction and the judicial gelding of class actions."[351]

Gilles and Friedman deftly illustrate that the drafters of PAGA made a series of grave errors in designing the law—rendering it unnecessarily susceptible to private enforcement's shortcomings.[352]

Take Article III first. PAGA employs the assignment model and vests the relator with far more power and control than the FCA. "[C]ourts have observed that PAGA suits are different from qui tam actions under the False Claims Act in that an aggrieved employee has complete control over his or her PAGA action."[353] Employing the assignment model in the new qui tam increases the likelihood that courts will hold that relators lack Article III standing.[354] The assignment model makes sense when the government suffers a property injury—with fraud being a quintessential example. But the new qui tam—like early American qui tam—protects against violations of broad collective injuries. Adopting the assignment model in the new qui tam invites arguments that the government lacks the "damages claim" from *Stevens*.[355] And absent the property injury, the government may have no injury to assign to the relator. The FCA's assignment model supplied Stevens with standing because he alleged governmental fraud, but there is no assurance that the assignment model also supplies standing when the relator alleges a violation of a broader social imperative.

To avoid the conclusion that relators lack Article III standing, the new qui tam must therefore adopt the agency model. "Relators under the new qui tam," Gilles and Friedman urge, should be "agents in the true sense. Unlike PAGA, where the relator acts 'on behalf of' similarly aggrieved others, and even collects penalties for their benefit, the new

350 *Id.* at 514–18.

351 *Id.* at 516.

352 Gilles and Friedman's criticisms of PAGA have proved prescient: the Supreme Court held in 2022 that the California Supreme Court's interpretation of PAGA was partially preempted by the FAA. *See* Viking River Cruises, Inc. v. Moriana, 142 S. Ct. 1906, 1924 (2022).

353 Gilles & Friedman, *supra* note 41, at 522 (citing Nanavati v. Adecco USA, Inc., 99 F. Supp. 3d 1072, 1082–83 (N.D. Cal. 2015)). *But cf. Viking*, 142 S. Ct. at 1914 n.2 ("The extent to which PAGA plaintiffs truly act as agents of the State rather than complete assignees is disputed. . . . For purposes of this opinion, we assume that PAGA plaintiffs are agents.").

354 *See* Gilles & Friedman, *supra* note 41, at 523 ("[I]t would be a mistake for progressive legislators to take comfort from lower court cases suggesting that PAGA plaintiffs have standing . . . .").

355 *See* Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 773 (2000).

qui tam relator acts only for the government, to vindicate its public interests."[356] Gilles and Friedman argue that the "philosophy of the new qui tam . . . must be that the relator represents the *state*, in its law enforcement capacity, and no one else."[357]

The FAA poses a second problem. PAGA includes a "relator injury" requirement: only aggrieved employees are authorized to bring suit on behalf of themselves and other current and former employees.[358] This ensures that every relator with statutory standing under PAGA can be bound by a mandatory individualized arbitration clause. And under the Supreme Court's 2022 decision in *Viking River Cruises, Inc. v. Moriana*, aggrieved employee relators will be bound to arbitrate their own PAGA claims—and *only* their own PAGA claims.[359]

In *Viking*, the Court held that the FAA preempted PAGA's claim joinder rule—the ability of one aggrieved employee to join her Labor Code violation claims with the Labor Code violation claims of other employees.[360] As a result, aggrieved employees bound by mandatory individualized arbitration clauses must resolve their own PAGA claims in bilateral arbitration and may not assert any other employee's PAGA claims in the arbitral forum.[361]

Since the *Viking* plaintiff was bound to arbitrate her own PAGA claims, the Court confronted the question of what to do with the claims the plaintiff had asserted on behalf of other aggrieved employees.[362] The Court—attempting to interpret California law—determined that "PAGA provides no mechanism to enable a court to adjudicate [other employees'] PAGA claims once an individual claim has been committed to a separate proceeding."[363] As a result, the Court concluded that the rest of the plaintiff's suit required dismissal.[364]

Viking thus guts PAGA as currently constituted: the employer successfully forced the plaintiff's own claim into arbitration, and the rest of her suit was dismissed.[365]

---

356 Gilles & Friedman, *supra* note 41, at 522–23 (footnote omitted).

357 *Id.* at 523.

358 *See* CAL. LAB. CODE §§ 2699(a)–(c) (West 2022).

359 *See* Viking River Cruises, Inc. v. Moriana, 142 S. Ct. 1906, 1924–25 (2022).

360 *See id.* at 1917–20.

361 *See id.*

362 *Id.* at 1925.

363 *Id.*

364 *Id.*

365 *See, e.g.*, Myriam Gilles, David Seligman, Andrew Elmore, Rachel Deutsch, Molly Coleman & Luke Norris, *Six Reactions to Viking River v. Moriana*, LPE PROJECT (June 29, 2022), https://lpeproject.org/blog/six-reactions-to-viking-river-v-moriana [https://perma.cc/Y453-D6DP] (Gilles: "[T]he ruling all but forecloses PAGA claims . . . .").

But surprisingly,[366] the Court did reject the employer's most aggressive argument—that courts should give effect to wholesale waivers of PAGA claims.[367]

In rejecting that broad contention, the Court arrived at two noteworthy holdings: first, the FAA does not require courts to enforce contractual waivers of substantive rights created under either state or federal law; and second, PAGA claims are materially distinguishable from class actions.[368] Together, these conclusions preserve a narrow path for states to employ representative enforcement schemes like the one proposed below.[369] Justice Sotomayor's concurring opinion explained that "the California Legislature is free to modify the scope of statutory standing under PAGA within state and federal constitutional limits."[370]

Viking thus illustrates at least some of the problems with PAGA's design. And while the decision could have proved disastrous for any future attempt at qui tam enforcement, the Court stopped short of allowing companies to unilaterally exempt themselves from all representative actions. In short, the case produced a narrow holding confined to PAGA's idiosyncrasies; a better-designed scheme can sidestep the whole morass.[371]

With these perils in mind, the next Section turns to the privacy qui tam proposal.

B. Privacy Qui Tam

Is privacy law amendable to Gilles and Friedman's vision for a new qui tam? After all, privacy has long been considered an individual, fundamental right. If avoiding PAGA's pitfalls necessitates articulating a broad social injury, can privacy possibly fit the bill? This Section first shows that scholars have long argued that privacy is a social

366 *See, e.g.*, *id.* (Elmore: "[I]n *Viking River*, the Supreme Court did something unexpected. It rejected the employer's argument that PAGA is a class action in disguise controlled by *Concepcion* and *Epic Systems*.").

367 *See Viking*, 142 S. Ct. at 1924–25.

368 *See id.* at 1919 n.5; *id.* at 1919–21.

369 *See* Gilles et al., *supra* note 365 (Seligman: "Most importantly, *qui tam* or whistleblower enforcement mechanisms remain viable paths for ensuring that states can enforce their laws without having to quadruple their enforcement budgets. States may delegate to workers, even those covered by arbitration provision, the right to assert claims on behalf of the state.").

370 *Viking*, 142 S. Ct. at 1925–26 (Sotomayor, J., concurring).

371 *Cf.* Will Baude & Dan Epps, *COBRA*, DIVIDED ARGUMENT, at 1:11:52 (June 19, 2022), https://dividedargument.com/episodes/cobra [https://perma.cc/HG6M-EZX4] ("[T]he Supreme Court ends up saying California could have a regime in which [the plaintiff] litigates the claims of a bunch of other people under state law as a representative of the state.").

phenomenon and then, in light of those insights, articulates the specifics of a privacy qui tam proposal.

1. Social Theories of Privacy

The oldest and most prominent articulation of the relationship between law and privacy is that the former should recognize the latter as an individual right. Samuel Warren and Louis Brandeis's famous article, *The Right to Privacy*, posited that privacy was the "right to be let alone" in the face of technological advancement that made "solitude" and "retreat from the world" more difficult than ever before.[372] This conception—of privacy as a right that belongs to an individual—has deep roots in liberal commitments to a self-determined autonomous individual, and as a result, it has had an enduring and enormously influential legacy in American law.[373]

More recently, however, scholars have argued that privacy as an individual right is actually an incredibly narrow conception of a broader social phenomenon with multiple sophisticated dimensions.[374] Privacy encompasses a host of different and related interests, which Daniel Solove calls a family resemblance—a group of concepts that draw from a common pool of similar elements, but which lack a single common denominator.[375] Trust, integrity, dignity, and space for the work of self-making are just a small handful of broader interests and social imperatives that fall under the umbrella term "privacy."[376] Recast in this light, privacy becomes vital to "social functioning: individual privacy guarantees enable collective values to flourish by making space for individuals to live freely, interact unreservedly, and participate fully in social life."[377] Privacy, in other words, isn't just freedom from the intrusions of others. Instead, privacy should be understood as a social phenomenon—one that produces desirable downstream consequences and protects a host of important interests.

Julie Cohen has argued that the "self who benefits from privacy is not the autonomous, precultural island that the liberal individualist model presumes," and privacy cannot "be reduced to a fixed condition or attribute (such as seclusion or control) whose boundaries can be

372 *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 196 (1890).

373 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 13–25 (2018).

374 *See, e.g.*, *id.* at 34–45; *see also* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 653 (2021); Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023).

375 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 9 (2008).

376 *See infra* notes 378–91 and accompanying text.

377 Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 559 (2020).

crisply delineated by the application of deductive logic."[378] Instead, privacy "is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development."[379] So understood, privacy is a resource necessary for human flourishing; its degradation through "the unchecked ascendancy of surveillance infrastructures" will produce a society that "cannot hope to remain a liberal democracy."[380]

Helen Nissenbaum has developed a theory of privacy called contextual integrity.[381] Nissenbaum observes that "[w]hat people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*."[382] Privacy as contextual integrity "makes rigorous the notion of appropriateness" by looking to "context-relative informational norms."[383] "When these norms are contravened," she explains, "we experience this as a violation of privacy."[384] These entrenched informational norms are, of course, socially constructed,[385] so privacy violations are derivatives of a collective tapestry of norms and expectations.

Ari Waldman has argued that privacy is "not about separating from society, but rather about engaging with it on terms based on trust."[386] We use trust, he explains, "to contextually manage our personae and the flow of our information in order to engage in social life."[387] Accepting the harmonious and dependent relationship between privacy and society reveals that privacy is "really a trust-based social construct between social sharers."[388] Privacy law, he argues, "should be focused on protecting and repairing the relationships of trust that are necessary for disclosure" and for engagement in social life.[389]

Solon Barocas and Karen Levy have illustrated how privacy is ultimately dependent upon the decisions of others.[390] Tie-based dependencies reveal information through a person's social relationships with others; similarity-based dependencies reveal information through

378 Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013).
379 *Id.*
380 *Id.* at 1911–12.
381 *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2 (2010).
382 *Id.*
383 *Id.* at 127.
384 *Id.*
385 *See id.* at 134–35.
386 WALDMAN, *supra* note 373, at 149.
387 *Id.*
388 *Id.*
389 *Id.*
390 *See* Barocas & Levy, *supra* note 377, at 556.

drawing inferences about a person's similarities to others; and difference-based dependencies reveal information about a person by process of elimination, ranking against others, and nonconformance.[391] Their taxonomy exposes privacy's interdependent nature—a reality to which atomized privacy is unresponsive.

These are just a small sampling of the rich theoretical reimagining of privacy as a social phenomenon—one that cannot be distilled into a negative right that belongs exclusively to individuals. So if our purpose is to determine whether privacy is amendable to qui tam enforcement using the agency model—a scheme that requires a public right enforceable by the government—the answer is unquestionably yes.

In fact, it's not just that privacy-as-a-social-phenomenon is plausible; these scholars have shown that it is vital and complementary way of understanding what privacy is. Only through adopting a social lens—and accepting that privacy invasions are a broad social injury capable of public enforcement—can we make sense of the observed shortcomings with privacy law today: foisting the responsibility for protecting privacy onto individuals and expecting them to make wise decisions when inundated with cumbersome cookie banners and indecipherable terms of service is how we produced a world where pervasive profit-driven surveillance is routine and where privacy is considered quaint, outdated, costly, and valued only by the persnickety. Recognizing privacy as a social phenomenon is the first crucial step in forging a legal and regulatory regime that is capable of valuing privacy and all its desirable effects.

2. Proposal

With that understanding of privacy as a social phenomenon in hand, the specific contours of a privacy qui tam proposal come into focus. This discussion addresses six considerations: purposes and findings, scope, process and model, penalties and remedies, differences between federal and state strategies, and severability.

a. Purposes & Findings

The authorizing legislation should begin with a robust articulation of the law's purposes and findings. "A statement of purpose would presumably reflect the expectation that statutory incentives will encourage private parties to recover civil penalties for the government that otherwise may not have been successfully assessed by overburdened . . . enforcement agencies."[392] Here, the legislature should

391 *See id.* at 559.

392 Gilles & Friedman, *supra* note 41, at 512.

explicitly endorse a social theory of privacy and explain that the statute is intended to protect privacy as a collective right. Adopting a social theory of privacy is essential to ensuring that relators have Article III standing and to fortifying the proposal against arguments that it constitutes an exotic and unprecedented use of qui tam.

b. Scope

The authorizing legislation should provide that "any person" acting in the public interest has authorization to bring a qui tam action under the law. In other words, the law should eschew a relator injury requirement. Similarly, the statute should studiously avoid any suggestion that the relator's compensation is intended to remedy a personalized injury or that the relator represents other aggrieved parties.

c. Process & Model

Like the FCA, the statute should require the relator to provide the government with a copy of the complaint and file it concurrently in court.[393] Also like the FCA, the law should give the government sixty days to decide whether to intervene.[394] And like the FCA, the statute should require the government's response one way or another—informing the court that the government has elected to intervene or notifying the court that the relator has the right to pursue the action in the government's name.[395]

Taking another cue from the FCA, the statute should use a "good cause" standard to limit the government's ability to request an extension and to reverse a nonintervention decision.[396] These limits are at least partially responsible for arguments that the FCA violates the Take Care Clause and Appointments Clause of Article II.[397] To minimize the threat that Article II poses to the proposal, a federal privacy qui tam should provide that the executive branch may remove the relator only upon a showing of good cause. Doing so conforms with the agency model—since the relator stands in the government's shoes to prosecute the action, the relator cannot have the exclusive and nonreversible authority to pursue the action. It's quite likely that such a structure—enacted inside or outside the qui tam context—would provoke the current Court to conclude that the statute violates Article II.[398]

393 *See* 31 U.S.C. § 3730(b)(2) (2018).
394 *See id.*
395 *See id.* § 3730(b)(4).
396 *See id.* §§ 3730(b)(3), (c)(3).
397 *See infra* subsection III.D.3.
398 *See infra* subsection III.D.3; *see also supra* note 321.

Ensuring that the relator is ultimately subject to the President's supervision minimizes the Article II objections.

The statute should then explicitly adopt the agency model and should disclaim the assignment model. The law should therefore seize on the Court's specific language about the agency model from *Stevens*. Under this privacy qui tam, the relator is "simply the statutorily designated agent of the [government], in whose name . . . the suit is brought—and that the relator's bounty is simply the fee he receives out of the [government's] recovery for filing and/or prosecuting a successful action on behalf of the Government."[399]

Adopting the agency model and disclaiming the assignment model has several effects that the legislature should enumerate. First, the statute should explain that if the government chooses to intervene, the relator has no right to continue as a participant in the litigation.[400] Second, if the government elects to intervene, the relator has no right to contest the government's later decision to voluntarily dismiss the suit.[401] And third, if the government intervenes, the relator has no right to demand a judicial determination on the fairness, adequacy, and reasonableness of the settlement.[402]

These three limitations have obvious drawbacks. They provide the government with the discretion to intervene in the suit and immediately terminate it—through voluntary dismissal with prejudice or through a nominal settlement that gives the defendant the benefit of res judicata. In times and places where the executive branch is led or captured by the surveillance industry's allies, this discretion is likely to frustrate the purpose of the statute. But these provisions are necessary, some judicial oversight may still be possible, and others can still fill the void they leave.

These limitations on the relator's involvement are necessary because giving the relator greater control over the suit is inconsistent with the agency model. Under common-law agency principles, an agent does not have the authority to prevent the principal from dismissing or settling litigation.[403] Scrupulously adhering to an agency model therefore necessitates embracing the government's ultimate authority to control the action and its resolution.

But just because the relator has no postintervention right to participate or contest dismissal and settlement doesn't mean the

399 Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 772 (2000) (emphasis omitted).

400 *Cf.* 31 U.S.C. § 3730(c)(1) (2018).

401 *Cf. id.* § 3730(c)(2)(A).

402 *Cf. id.* § 3730(c)(2)(B).

403 *Cf.* RESTATEMENT (SECOND) OF AGENCY § 1 (1958) (defining an agency relationship as including, *inter alia*, the principal's right to control the agent).

government's discretion is unlimited. One possibility is to vest oversight of settlements exclusively with the judiciary, rather than confer a contestation right on the relator. Because settlements can have preclusive effect, the law should grant the judiciary sua sponte authority to determine whether a nominal settlement is "fair, reasonable, and adequate"[404] or otherwise in the public interest. The executive's decision to voluntarily dismiss a suit, however, is subject to little or no oversight.[405] One ramification of adopting the agency model—and the related need to minimize Article II objections—is that neither the relator nor the judiciary can compel the government to continue an enforcement action if the government wishes to dismiss it. The judiciary should nevertheless retain the authority to determine whether the voluntary dismissal is with or without prejudice.

Finally, as discussed more below, privacy qui tam should be pressed at the federal and state level. If the federal government abuses these limits on the relator's involvement, states can still fill the void.

d. Penalties & Remedies

The statute should authorize the disgorgement of profits as a penalty.[406] To be most effective in the privacy context, the statute should not rely on inherent judicial disgorgement authority or require a standard of traceable economy injury.[407] Instead, the disgorgement authority should be tied to violations of the law's substantive standards and proscriptions.[408] The statute "should clearly prescribe disgorgement as a remedy for such violations, and it should empower regulators to define—and justify to the public—mechanisms for attributing profits to lawbreaking and for calibrating recovery based on order of magnitude effects."[409]

As for the relator's share, the statute should mostly adopt the FCA's structure: the relator receives a smaller share if the government

404 *Cf.* FED. R. CIV. P. 23(e)(2); 31 U.S.C. § 3730(c)(2)(B) (2018).

405 *Cf.* Swift v. United States, 318 F.3d 250, 252 (D.C. Cir. 2003) ("It may be that despite separation of powers, there could be judicial review of the government's decision that an action brought in its name should be dismissed. . . . But we cannot see how § 3730(c)(2)(A) [of the FCA] gives the judiciary general oversight of the Executive's judgment in this regard." (citing United States v. Cowan, 524 F.2d 504 (5th Cir. 1975))).

406 *See* COHEN, *supra* note 12, at 19.

407 *See id.*

408 *See id.*

409 *Id.* (first citing Paul Ohm, *Regulating at Scale*, 2 GEO. L. TECH. REV. 546, 554–55 (2018); and then citing Samuel N. Liebmann, Note, *Dazed and Confused: Revamping the SEC's Unpredictable Calculation of Civil Penalties in the Technological Era*, 69 DUKE L.J. 429 (2019)).

intervenes and a larger share (plus reasonable attorney's fees and costs) if the government declines to intervene.[410]

There are, however, two points of departure from the FCA. First, the statute should specifically provide that "the relator's bounty is simply the fee he receives out of the [government's] recovery for filing and/or prosecuting a successful action on behalf of the Government."[411] This again reinforces the statute's adoption of the agency model. Second, the statute should depart from the FCA in intervention cases. Under the FCA, relators in intervention cases receive between fifteen and twenty-five percent of the proceeds, but relators in FCA actions continue to participate in the action—hence why their bounties depend on the extent to which they contribute to the prosecution of the action.[412] That contribution language is inapposite in the privacy qui tam since it adopts the agency model. And because privacy qui tam relators have no residual role in the action—and since the disgorgement of profits may mean large penalties—a minimum of fifteen percent may prove to be a significant windfall for a relator who merely files the complaint. Policymakers may therefore favor a lower range or confer authority on the judiciary to determine a reasonable fee.[413]

e. Federal vs. State

Another consideration is the difference between privacy qui tam enforcement at the state and federal levels. To be most effective, privacy qui tam should be pursued at both. Doing so ensures that, even if the federal executive branch acts as an obstacle by intervening and dismissing or settling meritorious claims, concurrent state actions will continue apace.[414]

Several additional options, however, are available at the federal level. For example, a federal privacy qui tam should include an explicit FAA carve-out, which isn't an available strategy at the state level. Second, the federal initiative could similarly provide for an express

410 *See* 31 U.S.C. § 3730(d)(1)–(2) (2018).

411 Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 772 (2000) (emphasis omitted).

412 *See* 31 U.S.C. § 3730(d)(1) (2018).

413 For similar reasons, policymakers could also decide to lower the range even in non-intervention cases—down from the FCA's twenty-five to thirty percent—though receiving one-third of the recovery for having prosecuted the action is a well-accepted share. *See id.* § 3730(d)(2); *see, e.g.*, *Fees and Expenses*, AM. BAR ASS'N (Dec. 3, 2020), https://americanbar.org/groups/legal_services/milvets/aba_home_front/information_center/working_with_lawyer/fees_and_expenses [https://perma.cc/6VG3-P6J8].

414 *See, e.g.*, Gilles & Friedman, *supra* note 41, at 491 (urging a state law qui tam approach to compensate for federal abdication); Alexander, *supra* note 41, at 1203 (urging a state law qui tam response to *Concepcion*).

exemption from the strictures of Rule 23, ensuring that judges have no plausible path for grafting class action requirements onto a relator's action. Finally, statutes at both levels could explicitly identify the statute's prohibitions as protecting a public right to privacy—heading off any lingering Article III objections.[415]

At the state level, the calculus shifts. A state statute could explicitly exclude any person bound by a contract with the defendant from bringing the action—a potentially unnecessary provision that nevertheless ensures the action remains outside the scope of even the most muscular interpretation of the FAA.[416] Executive oversight of the action may also be more limited at the state level. Because the Take Care and Appointments objections are grounded in the Federal Constitution, states may have more room to vest the relator with sole and irreversible authority to pursue the action following the government's nonintervention decision.

f. Severability

Finally, statutes at both levels should make liberal use of severability clauses. Should the judiciary decide that one or more provisions of the privacy qui tam violate the Constitution, extremely detailed severability clauses increase the likelihood that the rest of the statute remains in effect.[417] It would hardly be surprising if the Supreme Court concluded that one or more of the provisions discussed above—like limiting the Executive's ability to reverse a nonintervention decision or the judicial oversight of the executive's settlement decisions—violate Article II.[418] Ensuring that these provisions can be severed from the rest of the statute will mean that the law's most vulnerable provisions do not doom the entire regulatory structure.

* * *

Qui tam's hybrid enforcement model has an untapped ability to avoid the shortcomings with public and private enforcement. The rest

415 *Cf.* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 301(c)(3) (2019) ("A violation of this Act or a regulation promulgated under this Act with respect to the covered data of an individual constitutes a concrete and particularized injury in fact to that individual."); Banning Surveillance Advertising Act of 2022, H.R. 6416, 117th Cong. § 3(c)(1)(C) (2022) ("A violation of this Act or a regulation promulgated under this Act with respect to the personal information of an individual constitutes a concrete and particularized injury in fact to that individual.").

416 *See infra* notes 420–25 and accompanying text.

417 *See, e.g.*, Will Baude & Dan Epps, *Triple Bank Shot*, DIVIDED ARGUMENT, at 13:54 (June 18, 2021), https://dividedargument.com/episodes/triple-bank-shot [https://perma.cc/P3JW-V4LX] (discussing how severability provisions could be improved).

418 *See infra* subsection III.D.3.

of this Part justifies the specifics of the privacy qui tam proposal just described.

C. Virtues

The privacy qui tam proposed above solves many of the problems with public and private enforcement detailed in Sections II.A and II.B, it avoids PAGA's mistakes covered in subsection III.A.2, and it operationalizes social theories of privacy reviewed in subsection III.B.1.

1. Public Enforcement

The proposal addresses the shortcomings with public enforcement detailed in Section II.A.

The qui tam's hybrid form of action addresses the widespread phenomenon of underenforcement. Relators don't rely on legislative appropriations to fund their activities. In fact, the proposal may strengthen public enforcement in two ways: First, relators' successful enforcement actions should generate revenue, and that revenue should be reinvested in public enforcement agencies like the FTC and California Privacy Protection Agency. Second, empowering relators saves regulators' time and money and thus allows agencies to expend these new resources on things other than ex post enforcement litigation, like rulemakings, monitoring, and other initiatives.

Relators are also not subject to political forces in the same way that agencies are. As private individuals, legislators have limited ability to browbeat and humiliate them, thereby eliminating the long-tail implications of an episode like KidVid. Nevertheless, there is lingering concern about political forces influencing intervention decisions. This is, however, an unavoidable problem with adopting a strong agency model. A multifaceted approach—pursuing privacy qui tam actions at the federal and state levels—helps ameliorate politics' sway on enforcement. And there can be little doubt that politicized enforcement decisions are already exacting a toll on robust privacy enforcement,[419] so it's doubtful the proposal will do anything other than improve the status quo.

And there is little concern about relators being captured by industry. The purpose of plenary enforcement authority—in the form of an "any person" agency model and pursuing the proposal in both statehouses and Congress—is that it's inherently fail-safe. Should one

419 *See, e.g.*, Ian Sherr, *Facebook's FTC Settlement Delayed by Political Infighting, Report Says*, CNET (May 24, 2019, 1:35 PM), https://cnet.com/news/facebooks-ftc-settlement-delayed-by-political-infighting-report-says/ [https://perma.cc/YF46-B9EN].

relator or one executive branch stand as an obstacle, others will fill the void.

Finally, aside from solving underenforcement, the proposal should also prove far more effective at shifting incentives and producing compliance than current law. Increasing the likelihood of being sued for violating the law becomes a near certainty, rather than today's haphazard enforcement that only targets a small number of egregious violators. And equally important is the form of the penalty: authorizing disgorgement addresses the ongoing problem that current enforcement actions are widely considered a necessary cost of doing business.

2. Private Enforcement & Other Qui Tam Enforcement

Three doctrinal impediments to effective private and qui tam enforcement surfaced in Section II.B and subsection III.A.2: adhesion contracts, Article III standing, and Federal Rule of Civil Procedure 23. This subsection explains how the proposal overcomes these hurdles.

First is the Federal Arbitration Act. For nearly twenty years, the unanimous opinion of the lower federal courts was that FCA claims were not subject to arbitration under the FAA.[420] This conclusion is intuitive, given what we've already seen about FCA claims—that they belong to the government. As the Ninth Circuit put it recently, "though the FCA grants the relator the right to bring a FCA claim on the government's behalf, an interest in the outcome of the lawsuit, and the right to conduct the action when the government declines to intervene, . . . the underlying fraud claims asserted in a FCA case belong to the government and not to the relator."[421]

But district courts in recent years have read the Supreme Court's writing on the wall and begun to send FCA claims to arbitration when they are asserted by employees subject to arbitration clauses.[422] In doing so, they have adopted a uniform rationale: "[Although] a qui tam suit is 'brought in the name of the Government,' [the action] still represents a claim belonging to the [p]laintiffs themselves.'"[423] PAGA

420 *See* Mathew Andrews, *Whistling in Silence: The Implications of Arbitration on Qui Tam Claims Under the False Claims Act*, 15 PEPP. DISP. RESOL. L.J. 203, 206 (2015).

421 United States *ex rel.* Welch v. My Left Foot Child.'s Therapy, LLC, 871 F.3d 791, 800 (9th Cir. 2017).

422 *See, e.g.*, Andrews, *supra* note 420, at 214–16 (discussing Deck v. Mia. Jacobs Bus. Coll. Co., No. 12-cv-63, 2013 WL 394875 (S.D. Ohio Jan. 31, 2013); Cunningham v. Leslie's Poolmart, Inc., No. CV 13–2122, 2013 WL 3233211 (C.D. Cal. June 25, 2013)).

423 *Id.* at 215 (quoting *Deck*, 2013 WL 394875, at *6–7).

claims have similarly proven susceptible to arbitration clauses.[424] As discussed above, the relator-injury requirement ensures that everyone capable of bringing a PAGA claim—and everyone on whose behalf the claim is brought—may be subject to an arbitration agreement.[425]

The specific contours of the proposal minimize the FAA's threat. Eschewing a relator-injury requirement, employing the agency model, and authorizing any person to sue in the public interest are all features that specifically reduce the proposal's susceptibility to FAA arguments. Indeed, *Viking* confirms that states have the authority to enact qui tam enforcement schemes that avoid FAA preemption.[426] And depending on where the proposal is implemented, legislatures have additional options available to further bolster the law's ramparts: at the federal level, Congress should include a specific FAA carveout,[427] and state legislatures could specifically withhold qui tam enforcement authority from anyone contractually bound to a defendant.

Second is Article III standing. The proposal sidesteps the Court's recent concrete injury decisions, which apply only to private rights of action. Even so, lingering standing objections have influenced the specific contours of the proposal. Because privacy harms will often be insufficiently concrete for a private right of action, the proposal eschews the assignment model, which may only be permissible in cases—like *Stevens*—where the government has suffered a property injury. Eschewing assignment means embracing agency. And as Gilles and Friedman have shown, the agency model fits best when the legislature articulates a broad social imperative or collective injury. Because there is little doubt the government could bring enforcement actions to pursue the public interest against structural privacy harms, there should be little room for the argument that the government cannot also designate private agents to bring these enforcement actions.

Along the way, social theories of privacy also place the proposal comfortably within qui tam's historical tradition. The rich, centuries-long tradition of qui tam enforcement of collective injuries—and the Court's explicit endorsement of relator standing in *Stevens*—makes it more difficult for the Court to reverse course and hold that relators in the agency model lack Article III standing.

---

424 *See, e.g.*, Viking River Cruises, Inc. v. Moriana, 142 S. Ct. 1906, 1925 (2022); Zenelaj v. Handybook Inc., 82 F. Supp. 3d 968, 979 (2015); Martinez v. Leslie's Poolmart, Inc., No. 14-cv-01481, 2014 WL 5604974, at *5 (C.D. Cal. Nov. 3, 2014).

425 *See supra* notes 358–65 and accompanying text; Gilles & Friedman, *supra* note 41, at 529–30.

426 *See Viking*, 142 S. Ct. at 1925–26 (Sotomayor, J., concurring).

427 *See, e.g.*, Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act of 2021, Pub. L. No. 117–90, 136 Stat. 26, 26–27 (2022) (codified as amended at 9 U.S.C. § 402(a)).

Finally, qui tam enforcement, if designed carefully and correctly, can avoid the shortcomings associated with class actions and Rule 23. PAGA's peculiar design invites arguments that it's just an attempt to provide class-wide relief without following the strictures of Rule 23. While the Supreme Court may have distinguished between PAGA actions and class actions in *Viking*,[428] other courts have embraced the analogy.[429] As a result, the privacy qui tam proposal eschews class-like devices: the relator brings a claim—standing in the shoes of the government—to remedy a societal privacy injury, and there is no relief distributed to anyone whose privacy may have been affected by the defendant's conduct. Instead, the relator receives a portion of the government's award as a bounty and the rest of the penalty is remitted to the government, ideally earmarked for further enforcement matters. Because the relator is an agent of the government, the relator's Article III standing is premised on the government's authority to protect and promote the public interest. And because there is no relator-injury requirement and the proposal does not attempt to distribute relief to other affected or aggrieved individuals, there is no need for district courts to agonize over whether a class is ascertainable or whether plaintiffs' claims satisfy the commonality and predominance requirements of Rule 23.

3. Operationalizing Privacy Theory

Finally, one of the proposal's strengths is that it operationalizes privacy scholarship's insight that privacy is a social phenomenon best protected at the societal level. Others and I have frequently argued that privacy rights and privacy harms should be individually enforceable to circumvent the gridlock associated with public enforcement.[430] But these arguments and proposals tend to repeat one of the errors that has produced the current state of affairs—placing the responsibility to protect a public value onto the backs of individuals. At the same time, it's indisputable that public enforcement has not and cannot keep pace with information capitalism's rapid production of new and highly profitable business models that generate new and novel harms. Closing the enforcement gap using qui tam seizes on the best features of both public and private enforcement.

428 *See Viking*, 142 S. Ct. at 1919–21.

429 *See* Gilles & Friedman, *supra* note 41, at 520–21, nn.156–57 (collecting cases).

430 *See, e.g.*, Citron & Solove, *supra* note 270, at 821; Ormerod, *supra* note 62, at 1894. *See generally* Ormerod, *supra* note 236.

D. Criticisms

The proposal is not immune to criticism, and three types of objections are worth confronting directly.

1. Implausible & Unprecedented

The first type of objection is that the proposal is implausible. This objection can take several forms. One version focuses on the judiciary: the critic argues that it's naïve to assume that federal courts will uphold an exotic and unprecedented enforcement scheme. Another focuses on the legislature, contending that Congress and state legislatures are certain to recoil at a law that invites such litigiousness. A third points to industry opposition: the neoliberal framework and resulting regulatory capture would surely neuter the proposal's effectiveness, even if it were enacted. Yet another seizes on the sorry state of privacy law today to posit that privacy isn't really a social good that requires a policy intervention at all.

These objections are all versions of an argument sometimes called the inside/out fallacy. With the inside/out fallacy, "the diagnostic sections of a paper . . . offer deeply pessimistic accounts of the ambitious, partisan, or self-interested motives of relevant actors in the legal system, while the prescriptive sections of the paper then turn around and issue an optimistic proposal for public-spirited solutions."[431] In other words, this category of objections points to the pessimistic account of the status quo articulated in Parts I and II and argues that this account cannot be squared with the rosy optimism necessary for the proposal to work as intended.

There can be little doubt these objections have persuasive force. The proposal has, however, been specifically crafted to counteract concerns that it too will be subsumed by the machinery of information capitalism.

The judiciary-focused critique proves too much. Scholars have begun recognizing the power and importance of qui tam,[432] and the proposal builds on this foundational work. It's modeled after qui tam enforcement of collective injuries from the seventeenth and eighteenth centuries, and it departs from the FCA and PAGA in specific and intentional ways for the purposes of bolstering the statute's effectiveness. A proposal that fell victim to the inside/out fallacy would look rather

431 *See* Eric A. Posner & Adrian Vermeule, *Inside or Outside the System?*, 80 U. CHI. L. REV. 1743, 1745 (2013).

432 *See generally* Will Baude & Dan Epps, *Inner Sanctum*, DIVIDED ARGUMENT, at 31:07 (July 27, 2021), https://dividedargument.com/episodes/inner-sanctum [https://perma.cc/8GRB-E7J5]; Gilles & Friedman, *supra* note 41; Alexander, *supra* note 41; Elmore, *supra* note 41.

different; nearly every aspect of the statute outlined in subsection III.B.2 has the purpose of minimizing or avoiding pitfalls associated with other attempts to privately enforce legal rights. The proposal recognizes that the same doctrines undermining private enforcement also threaten qui tam enforcement, and it seizes on favorable precedents and historical arguments precisely because failing to do so invites the judiciary to invalidate the scheme or gut its effectiveness. If the courts are determined to protect informational businesses' profits—beyond any commitment to settled doctrine—it's not clear that any attempt to address privacy harms could succeed.

A legislative response is also more likely than the critic assumes. It's of course true that any federal policy proposal faces an uphill battle in Congress. But Gilles and Friedman explain that the new qui tam has a real chance of success at the state level.[433] Colorado, for example, recently included a qui tam enforcement scheme in a state workplace health and safety law.[434] Continued political gridlock at the federal level is always a good bet, but a qui tam proposal may be able to shift the terms of the debate,[435] and there are some indications of bipartisan momentum on privacy law.[436]

Capture concerns are also overstated. One virtue of the qui tam proposal is that it doesn't require ongoing appropriations like a public enforcer. Unlike most federal consumer protection, the proposal is a one-time authorization that farms out enforcement and thereby funds itself. One of qui tam's most appealing aspects is that it's considerably more difficult for industry and its political clients to capture and neuter than a centrally enforced scheme.

Finally, the fact the privacy is underprotected today can tell us very little about whether robust protection is warranted.[437] Social goods are often neglected, and privacy is no exception. There is a great deal of money to be made in the surveillance industry today, whereas its harms can be diffused and amorphous. The status quo shows that public enforcers will not and private enforcers cannot effectively enforce privacy law; it cannot tell us whether individuals would choose to enforce privacy law if given the opportunity. The proposal gives individuals the

433 *See* Gilles & Friedman, *supra* note 41, at 531–35.

434 *See* COLO. REV. STAT. § 8-14.4-107 (2022).

435 *Cf.* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 403 (2022) (bipartisan data privacy bill that includes a severely limited private right of action, an arbitration carveout for minors, and some qui-tam-like enforcement provisions).

436 *See id.*; *see also* Peter Swire, *The Bipartisan, Bicameral Privacy Proposal Is a Big Deal*, LAWFARE (June 9, 2022, 2:12 PM), https://www.lawfareblog.com/bipartisan-bicameral-privacy-proposal-big-deal [https://perma.cc/3UG9-LLVW].

437 *See, e.g.*, DAVID HUME, A TREATISE OF HUMAN NATURE 469 (L.A. Selby-Bigge ed., Oxford, Clarendon Press 1888) (1739) (articulating the is–ought problem).

opportunity to decide to what extent privacy law should be enforced—thereby effecting a democratization of privacy enforcement.

In sum, the proposal's *raison d'être* is that its defenses are fortified from attack by skeptical legislators, hostile judges, and a wealthy, organized, and motivated industry.

2. Alternatives

A second objection accepts that qui tam enforcement is a viable path forward for addressing the dual-forked shortcomings with public and private enforcement, but it nonetheless contests the need for a privacy-specific qui tam. Alternative strategies include a generally applicable consumer protection qui tam, antitrust regulation, and regulations aimed at platform power and content moderation problems.

The first version of this objection asks why policymakers should pursue a privacy-specific qui tam when a UDAP qui tam could provide broader relief for other types of objectionable business practices.[438]

Policymakers *should* pursue a generally applicable UDAP qui tam. Almost all the criticisms of the FTC above apply with similar or equal force to fields outside of privacy law.[439] A multipronged approach is necessary—and not just for privacy law. The neoliberal managerial mindset that pervades business regulation in the United States wasn't created overnight and will take a concerted approach to change.[440]

But policymakers should also pursue privacy-specific qui tam enforcement. Folding privacy harms under the umbrella of UDAP for the past thirty years has not proved effective. While much of that may be attributable to the FTC as an institution rather than the nature of its authority, there are good reasons for privacy to be treated differently from other consumer injuries. Deception tends to be rather limited—typically holding a defendant to its express representations—and unfairness has the checkered history detailed above.[441] Today, both sources of authority are rooted in violations of consumer expectations,[442] but conceiving of privacy injuries as only unwelcome consumer surprise is extraordinarily narrow and promises to further entrench the status quo. Both deception and unfairness authorities also include a consumer harm requirement.[443] As we've seen, tying privacy injuries to individual consumer experiences is a grave mistake that

438 *See, e.g.*, Alexander, *supra* note 41.

439 *See generally* Herrine, *supra* note 143.

440 *See, e.g.*, *id.* at 491–502; *see also* COHEN, *supra* note 74, at 7. *See generally* WALDMAN, *supra* note 20.

441 *See, e.g.*, WALDMAN, *supra* note 20, at 99–100.

442 *See* Solove & Hartzog, *supra* note 104, at 666–72.

443 *See* HOOFNAGLE, *supra* note 103, at 129 (deception); *id.* at 131–32 (unfairness).

produced the woefully inadequate notice-and-waiver regime we have today. Privacy cases are unique in that consumers truly are unable to protect and help themselves.[444] A *sui generis* problem calls for a bespoke solution.

Another version of this objection argues that antitrust is the best—and perhaps only—strategy for regulating large technology companies.[445] According to this objection, pursuing strategies other than antitrust is folly because of the opportunity costs and path dependence associated with one regulatory initiative over others.

Again, policymakers *should* pursue robust antitrust regulation, but procompetitive measures should not subsume all other regulatory strategies. Antitrust law in the past generation has proven remarkably susceptible to capture and market fundamentalism,[446] so there are reasons to doubt its responsiveness to the current environment.

But more fundamentally, antitrust regulation and privacy regulation are not substitutes. In fact, they can move in opposite directions because competition mandates can further extend data flows, compounding surveillance harms.[447] While antitrust scholars tend to suggest that competition law should be pursued to the exclusion of other regulatory strategies, accepting that premise would be a mistake. Even if antitrust can be resuscitated for the information age, its solutions are not necessarily responsive to surveillance-based harms.

A last version of this objection points to other types of harms, like content moderation and platform power.[448] But as we've just seen, specific problems call for specific solutions, and much contemporary debate about technology companies' power tends to falter at the starting gate because no one agrees on the problems that need solving.[449] Surveillance harms and platform-power harms share a cause—scale. But the harms themselves are distinct, and there can be no one-size-fits-all solution.

---

444 *See, e.g.*, Herrine, *supra* note 143, at 522.

445 *See, e.g.*, Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 537 (2019).

446 *See, e.g.*, Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 717–37 (2017).

447 *See* COHEN, *supra* note 12, at 11 ("Antitrust law has long grappled with the question of how to reconcile intangible intellectual property rights with competition mandates; addressing market domination within networked information ecosystems requires confronting similar questions about the appropriate extent of control over networked data flows structured by technical and legal protocols.").

448 *Cf.* Hannah Bloch-Wehba, *Content Moderation as Surveillance*, 36 BERKELEY TECH. L.J. (forthcoming 2022) (manuscript at 141), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872915.

449 *See* Mark A. Lemley, *The Contradictions of Platform Regulation*, 1 J. FREE SPEECH L. 303, 305 (2021).

3. Article II

A third objection argues that the proposal—adopted at the federal level—violates Article II of the Constitution. This is a serious objection, and defenders of the proposal must be prepared to overcome it.

In *Stevens*, the Supreme Court specifically reserved the question of whether the FCA violated Article II. In a footnote at the conclusion of its standing discussion, the majority explained: "[W]e express no view on the question whether *qui tam* suits violate Article II, in particular the Appointments Clause of §2 and the 'take Care' Clause of §3."[450] Addressing that question was not necessary, the Court explained, because Vermont had not raised it, and the "validity of *qui tam* suits under those provisions" was not "a jurisdictional issue" like Article III standing.[451] The dissent criticized the majority for mentioning the Article II objection, and the majority responded that "[w]e raise the question . . . only to make clear that it is not at issue in this case. It is only the dissent that proceeds to volunteer an answer."[452]

After *Stevens*, some have pressed the point explicitly.[453] There are good reasons to be concerned that stringent interpretations of both clauses are ascendant among the current Court. *TransUnion*'s discussion of Article II suggests that delegating law enforcement authority may violate the Take Care Clause,[454] and the Court has decided several important appointment and removal cases in recent years.[455]

According to the Court's Appointments cases, members of the executive branch fall into three categories: principal officers, inferior officers, and employees and contractors. Principal officers must be appointed through nomination by the President and consent of the Senate; Congress may provide for inferior officers to be appointed the same way or by the President alone, by the judiciary, or by cabinet secretaries; and employees and contractors are not subject to appointment restrictions because they are "lesser functionaries" that do not "exercise significant authority pursuant to the laws of the United States."[456] In 2021's *United States v. Arthrex, Inc.*, the Court concluded

450 Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 778 n.8 (2000).

451 *See id.*

452 *See id.* at 801–02 (Stevens, J., dissenting); *id.* at 778 n.8 (majority opinion).

453 *See, e.g.*, Kathryn Feola, Comment, *Bad Habits: The Qui Tam Provisions of the False Claims Act Are Unconstitutional Under Article II*, 19 J. CONTEMP. HEALTH L. & POL'Y 151, 164–85 (2002).

454 *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2207 (2021).

455 *See* Seila L. LLC v. Consumer Fin. Prot. Bureau, 140 S. Ct. 2183, 2211 (2020) (removal); United States v. Arthrex, Inc., 141 S. Ct. 1970, 1972 (2021) (appointment).

456 *See Arthrex*, 141 S. Ct. at 1978–80 (quoting Buckley v. Valeo, 424 U.S. 1, 126 & n.162 (1976) (per curiam) (alteration omitted)).

that the Administrative Patent Judges on the Patent Trial and Appeal Board were principal—and not inferior—officers, which meant that their method of appointment violated the Appointments Clause.[457] Administrative Patent Judges are principal officers, the Court explained, because they "have the 'power to render a final decision on behalf of the United States' without any such review by their nominal superior or any other principal officer in the Executive Branch."[458]

The Take Care Clause analysis follows a similar path. Congress's decision to protect members of the executive branch with for-cause removal restrictions, the Court has said, can violate the separation of powers. For example, the Court held in 2020's *Seila Law LLC v. Consumer Financial Protection Bureau* that "principal officers who, acting alone, wield significant executive power" must be removable by the President at will and may not be subject to a for-cause removal restriction.[459] But the Court has also held that for-cause removal restrictions do not violate the separation of powers when principal officers sit on a multimember commission or when the restriction applies to inferior officers.[460]

Lower courts have rejected Article II challenges to the FCA both before and after *Stevens*. The Ninth Circuit has held that FCA relators are neither principal nor inferior officers because they do not exercise significant executive authority and because "a qui tam relator, who litigates only a single case, does not have 'primary responsibility' . . . for enforcing the FCA."[461] Similarly, the en banc Fifth Circuit has held that the FCA violates neither the Take Care Clause nor the Appointments Clause because relators do not have a "continuing and formalized relationship of employment with the United States Government."[462] The Sixth and Fourth Circuits have reached the same conclusion.[463]

Despite the unanimity of the lower courts on these questions, *Seila Law* and *Arthrex* suggest that the current Court is particularly attuned

457 *Id.* at 1979–86.

458 *Id.* at 1981 (quoting Edmond v. United States, 520 U.S. 651, 665 (1997)).

459 *See Seila L.*, 140 S. Ct. at 2211.

460 *See* Jerry L. Mashaw, *Of Angels, Pins and For-Cause Removal: A Requiem for the Passive Virtues*, U. CHI. L. REV. ONLINE (Aug. 27, 2020), lawreviewblog.uchicago.edu/2020/08/27/seila-mashaw/ [https://perma.cc/CQ9C-Z4N6] (first citing Humphrey's Ex'r v. United States, 295 U.S. 602 (1935) (multimember commissions); and then citing Morrison v. Olson, 487 U.S. 654 (1988) (inferior officers)).

461 *See* United States *ex rel.* Kelly v. Boeing Co., 9 F.3d 743, 757–59 (9th Cir. 1993).

462 *See* Riley v. St. Luke's Episcopal Hosp., 252 F.3d 749, 753–58 (5th Cir. 2001) (en banc).

463 *See* United States *ex rel.* Taxpayers Against Fraud v. Gen. Elec. Co., 41 F.3d 1032, 1041 (6th Cir. 1994); United States *ex rel.* Milam v. Univ. of Tex. M.D. Anderson Cancer Ctr., 961 F.2d 46, 49 (4th Cir. 1992).

to political accountability in the executive branch.[464] As a result, a federal privacy qui tam statute should give the executive branch at least as much authority over the actions as the FCA, and the proposal detailed above is specifically designed to minimize Article II objections. Under the proposal, the relator should not be considered a principal or inferior officer and may therefore be protected by a for-case removal standard.

A federal privacy qui tam would be more potent if it granted the relator the exclusive and irreversible authority to pursue the action after the government declines to intervene.[465] But the proposal must avoid resembling a statute that grants authority to someone to pursue cases in the executive branch's name without any oversight from the President.[466] While the sixty-day intervention period means that the qui tam proposal is not that strong—since the executive branch has the unfettered authority to intervene at the outset—a structure that totally prohibits the government from reversing its earlier nonintervention decision starts to look similar once those sixty days have elapsed. Protecting the relator only through for-cause removal has obvious drawbacks and does not ensure that the Court will uphold the statute, but it does minimize the risk because the President retains ultimate authority over the action. In the end, however, employing robust severability provisions and pursuing a concurrent state-law strategy ensure that this objection cannot prove fatal.

CONCLUSION

Information capitalism in the twenty-first century generates extreme wealth while having little regard for its surveillance-related harms. Privacy law attempts to address this disparity by internalizing the costs that businesses pass onto society. Unfortunately, privacy law has thus far proven inept at doing so because it suffers from a failure of imagination across multiple dimensions. To date, policymakers have adhered to a strict notice-and-waiver regime, and they have ignored the reality that conventional enforcement schemes are ineffective.

Privacy scholars are attempting to supply those policymakers with new ideas for more effective legal regimes. This Article has furthered

464 *Cf.* Polansky v. Exec. Health Res. Inc., 17 F.4th 376 (3d. Cir. 2021), *cert. granted*, 142 S. Ct. 2834 (2022).

465 While executive oversight of qui tam claims invites capture-related abuses, *see supra* notes 393–98 and accompanying text, the government's gatekeeping authority may also have its own advantages, *see supra* notes 342–43 and accompanying text.

466 *Cf.* Morrison v. Olson, 487 U.S. 654, 706 (1988) (Scalia, J., dissenting); Swift v. United States, 318 F.3d 250, 252–53 (D.C. Cir. 2003).

that initiative by proposing a novel enforcement scheme that has a rich history and a great deal of promise. Qui tam can fill the enforcement void left by underfunded and disinterested regulators and by doctrines that have gutted private enforcement. Adopting a social theory of privacy and avoiding California's mistakes help ensure that a statute with qui tam enforcement will be vigorously enforced by enterprising relators and will not be subject to private actions' thicket of procedural and substantive obstacles.

Better privacy laws are possible, and qui tam shows that creative policymakers can promote the effective enforcement of privacy law.