Harvard Journal of Law & Technology
Volume 33, Number 1 Fall 2019

ENFORCING DIGITAL PRIVACY

*Brian Yost**

TABLE OF CONTENTS

I. INTRODUCTION

The near anarchy of digital privacy governance has come to a halt. Data breaches and widespread privacy violations have shown that the current regulatory landscape does not adequately protect consumers. More recent scandals have increased public urgency to address this problem. Equifax's 2017 data breach exposed 147 million Americans' personal data.[1] These millions may suffer identity theft, economic harm, and the autonomy injury of having sensitive information made public without their consent. And from 2014 through the 2016 U.S. presidential election, Cambridge Analytica illicitly harvested over 87 million Facebook user profiles and used this data to influence voting behavior.[2]

---

* Harvard Law School, J.D. 2019. I would like to thank Professor Urs Gasser for advising me on this Note's topic. I would also like to thank Alexandra Mushka and the other editors at the Harvard Journal of Law & Technology for all of their invaluable help in improving and publishing this Note.

1. *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Sept. 2019) https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [https://perma.cc/ZZ82-B9JQ].

2. *In re Facebook - Cambridge Analytica*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/facebook/cambridge-analytica [https://perma.cc/S5AC-LN34].

Responding to these and many other privacy scandals, governments unveiled sweeping privacy regulations. Most notably in 2016, the European Union ("E.U.") approved the General Data Protection Regulation ("GDPR"), which fundamentally altered how companies can process an E.U. individual's data.[3] Two years later, California enacted the California Consumer Privacy Act ("CCPA").[4] Once in force, the CCPA will regulate most aspects of data privacy and processing.[5] This contrasts sharply with the sectoral (and arguably deficient) federal privacy regime in the U.S.[6] At the federal level, several legislators have introduced omnibus privacy bills of varying scope.[7] Countless class action lawsuits have sought damages for privacy harms against this backdrop, but most have failed.[8]

The U.S., E.U., and California's disparate responses to privacy violations stem from difficulty in defining both privacy and its attendant harms. Privacy harms bridge the ethereal and the concrete, including both inherent privacy harms and concrete attendant harms arising from specific violations of individuals' privacy. This duality hamstrings legislatures and courts ill-prepared to combat information-age injuries. This Note proposes an enforcement regime that reflects this ethereal-concrete divide. In whichever substantive regulatory scheme legislators enact, they should bifurcate privacy enforcement to reflect this divide. Specifically, an enforcement regime should (1) empower the federal government to litigate statutory damages for inherent privacy harms and (2) restrict private litigation to resolving only the attendant injuries that result from privacy violations. The government would distribute to affected consumers the statutory damages, which would differ according to each distinct type of data unlawfully disclosed and the context in which the data was disclosed. Together, these elements resemble the

3. *See* Regulation 2016/679 of Apr. 27, 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 (EU).

4. *See generally* The California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.198 (West 2018).

5. *See id.*

6. *See* Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 324, 325–32 (Beate Roessler & Dorota Mokrosinska eds., 2015) (describing the sectoral and federalist aspects of U.S. privacy regulation).

7. *See* Consumer Data Protection Act, S. 2188, 115th Cong. (2018); Data Care Act of 2018, S. 3744, 115th Cong. (2018); American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019).

8. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012); *see also* Eric Goldman, *The Irony of Privacy Class Action Litigation*, 10 J. ON TELECOMM. & HIGH TECH. L. 309, 318 & n.47 (2012) (arguing that privacy class action suits frequently fail and often only enrich the plaintiffs' lawyers).

Medicare Physician Fee Schedule's ("MPFS") structure.[9] This granular, contextual approach aligns the penalties — and therefore compensation — with the privacy harm's severity. To avoid double recovery, only concrete attendant injuries flowing from a privacy violation would merit private litigation. Part II addresses this regime's theoretical and practical underpinnings. Part III details the regime's structure and why stakeholders might ultimately support it. Part IV concludes.

II. THE REGIME'S THEORETICAL AND PRACTICAL UNDERPINNINGS

Privacy has consistently eluded simple definition.[10] Privacy's attendant harms likewise strain against simple definition.[11] Consequently, this Note does not fully define privacy harm and instead employs an instrumental framework.[12] In particular, the regime bifurcates privacy enforcement. First, the government would enforce inherent privacy harms. Two complementary conceptualizations of privacy drive this prong's structure, which adopts a modified fee schedule for disclosing different types of data. This approach parallels both privacy theory and the U.S.'s sectoral approach to regulating privacy. Second, this regime allows a private party to litigate attendant harms that stemmed from violating her privacy only. This Part first illustrates how conceptualizing privacy harm as inherent or attendant supports bifurcating enforcement. It then explores the U.S.'s sectoral approach through the lens of "contextual integrity."[13] This exploration illustrates

---

9. *See* Medicare Program; Revisions to Payment Policies Under the Physician Fee Schedule, 83 Fed. Reg. 59,452 (Nov. 23, 2018) (to be codified at 42 C.F.R. pt. 400) (revising the MPFS); *see generally* CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE PHYSICIAN FEE SCHEDULE (2017), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/MedcrePhysFeeSchedfctsht.pdf [https://perma.cc/4C6C-25YX]; CTRS. FOR MEDICARE & MEDICAID SERVS., MEDICARE CLAIMS PROCESSING MANUAL: CHAPTER 12 - PHYSICIANS/NONPHYSICIAN PRACTITIONERS (2019), https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/clm104c12.pdf [https://perma.cc/9LS3-8PYX].

10. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479–80 (2006) (collecting examples of academics lamenting the lack of a clear definition of privacy); Judith Decew, *Privacy*, STAN. ENCYC. OF PHIL. (Jan. 18, 2018), https://plato.stanford.edu/entries/privacy [https://perma.cc/T473-BE7J] (detailing the "wide array of philosophical definitions . . . of privacy").

11. *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099–1124 (2002) (exploring different conceptualizations of privacy and the harms against which they guard); *cf.* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695–97 (7th Cir. 2015) (recognizing the increased risk of identity theft as conferring standing but expressing doubt that loss of private information characterized by plaintiffs as an "intangible commodity" could support standing).

12. *Cf.* Solove, *supra* note 10, at 481–82 (leaving privacy undefined in favor of proposing a taxonomy of privacy harms).

13. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136 (2004).

that sectoral privacy regulation implies that society values different data types differently. The penalties associated with these harms should vary accordingly.

A. A Dichotomy of Privacy Harms

This Note delineates privacy injuries into two distinct types: inherent privacy harms and attendant privacy harms arising from violations of one's privacy. The latter embraces definition more readily than the former. An attendant harm maps onto traditional privacy-related torts. One example is when phishing scammers steal one's identity or leak sensitive information damaging one's reputation. These (often economic) harms surmount Article III standing's hurdle relatively easily.[14] They mirror the sort of harm that the Supreme Court requires under *Spokeo, Inc. v. Robins*.[15] There, Spokeo, a people search engine, aggregated and disseminated partially inaccurate information about plaintiff Thomas Robins. Despite Spokeo arguably violating Robins' inherent privacy, the Court dismissed the claim.[16] Merely violating the Fair Credit Reporting Act did not confer standing.[17] Instead, standing required a concrete harm.[18] Similarly, courts have required manifest economic injury in many data breach class actions.[19] For example, in *Resnick v. AvMed*,[20] the court recognized the standing of data breach victims who suffered actual instances of identity theft.[21] Some courts, however, have conferred standing for the mere *potential* for identity theft.[22] While these decisions often still couch privacy harm in the lan-

14. *See, e.g.*, *Remijas*, 794 F.3d at 695–97 (concluding that data breach "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" conferred standing); Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc.), 870 F.3d 763, 771–72, 774 (8th Cir. 2017) (affirming dismissal of claims alleging risk of future identify theft but allowing claim alleging a fraudulent charge — i.e., present identity theft).

15. 136 S. Ct. 1540, 1544–45, 1549–50 (2016).

16. *Id.* at 1549–50.

17. *Id.*

18. *Id.* (discussing how "concrete" can encompass both tangible or intangible injuries, including injuries Congress has "elevat[ed] to the status of legally cognizable injuries"); *see also* Remijas, 794 F.3d at 695 (refusing to confer standing for the "abstract injury" to the plaintiffs' "intangible commodity" of private information).

19. *See* Kelsey Finch, *The Evolving Nature of Consumer Privacy Harm*, IAAP: THE PRIVACY ADVISOR (Apr. 1, 2014), https://iapp.org/news/a/the-evolving-nature-of-consumer-privacy-harm [https://perma.cc/TP6L-VQ95].

20. 693 F.3d 1317 (11th Cir. 2012).

21. *Id.* at 1323.

22. *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (concluding that the "credible threat of real and immediate harm stemming from" a data breach sufficiently constitutes Article III standing injury-in-fact). *But see, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (denying standing when the plaintiff alleged only an increased risk of a third party accessing information "unanchored to any actual incident of data breach").

guage of pocketbook injuries, they recognize that violating one's privacy and exposing one's data harms the individual even if a data breach does not manifest monetarily.

As these courts have begun to recognize, privacy harm exists beyond the purely economic. Inherent privacy harms have been characterized in a variety of ways. First, they may intrude upon one's "inviolate personality."[23] Second, they may create a less favorable "context for respect, love, friendship, and trust" to blossom.[24] Third, they may shrink one's "realm of intimacy" — a space necessary for forming and strengthening intimate relationships.[25] Fourth, the harms may violate the victim's informational autonomy?[26] Fifth, they might just instill in the victim the disconcerting feeling of a complete stranger ruffling through one's once private information. Focusing on a data breach's economic harm, consequences, or even resulting emotional distress fails to encapsulate privacy harm's nature. Another category, defined in this Note as an "inherent privacy harm," must exist — even if no one can agree on its definition.[27]

This Note's proposed incorporation of inherent privacy harm partially mirrors Ryan Calo's subjective-objective dichotomy.[28] Calo categorizes privacy harm in relation to its victim. Subjective harms manifest within the victim and stem "from the perception of unwanted observation."[29] This half of the privacy harm spectrum often inflicts emotional discomfort or distress.[30] Conversely, objective privacy harm exists solely external to the victim.[31] Calo predicates this harm on "the forced or unanticipated use of information about a person against that person."[32] This harm sweeps far more broadly than its counterpart. Objective harms include any instance in which private information facilitates an adverse action or crime against its subject.[33] Calo's delineation of privacy harms into distinct categories provides an effective tool to examine privacy harms.[34]

---

23. *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964)

24. CHARLES FRIED, AN ANATOMY OF VALUES 140 (1970).

25. JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 74–75 (1996).

26. *See* W. A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 269 (1983) ("Privacy is the condition of not having undocumented personal knowledge about one possessed by others.").

27. *Cf.* ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 5 (1988) ("There is no universally accepted philosophical definition of 'privacy.'").

28. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142–43 (2011).

29. *Id.* at 1142.

30. *Id.*

31. *Id.* at 1143.

32. *Id.*

33. *See id.*

34. *See id.* at 1153–54.

The regime proposed in this Note builds on Calo's categoric approach but narrows his subjective harm category to harm inherent to violating one's privacy. Where Calo's dichotomy hinges on the harm's relationship to the victim, this Note's dichotomy looks to the nature of privacy itself. Where Calo might vary privacy harm and enforcement by person, this Note's regime would not. Consequently, it diverges in two significant ways. First, the Note's "inherent privacy harm" does not incorporate fraught emotional states or exacerbated data misuse fears. By defining inherent harms more narrowly than subjective ones, the Note does not use or view privacy as a means to an end. If privacy stands as a fundamental right in itself, then using privacy only to protect one's emotional state degrades privacy's inherent importance. Further, this Note's definition avoids making harm relative to a victim's emotional constitution.

Second, the Note's inherent harm category is narrowed to a more universal, standardized harm. This would better allow courts to adjudicate large-scale privacy harms efficiently. If one viewed privacy harms subjectively, litigating a data breach would require analyzing every affected party's emotional vulnerability and injury. Although courts could average amounts of harm or employ heuristics, this would untether their analyses from Calo's "subjective harms." This narrow category of harm inheres to the injury to privacy itself. Under this theory, one would remediate true emotional distress as a harm flowing from violations of one's privacy. Consequently, an enforcement regime should explicitly redress violations of this inherent privacy right and compensate for objective harms flowing from the violation.[35] A European trend towards increasing damages for dignitary privacy harms supports this. Specifically, the European Court of Human Rights has shifted its punitive approach towards levying greater and greater damages for non-pecuniary harm.[36] These damages for non-pecuniary harm allow recovery for dignitary privacy harms, which closely mirror this Note's "inherent privacy harms." In order to give effect to its conception of inherent privacy harms, this Note proposes a system that centrally enforces statutory penalties for violating data privacy and curtails private litigation to attendant harms.

35. *Cf.* DesignerWare, LLC, 155 F.T.C. 421, 427 (2013) (alleging that tracking computer activity and visually monitoring individuals inflicted financial injury and "impair[ed] their peaceful enjoyment of their homes.")

36. Bart van der Sloot, *Where is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 322, 328–29 (2017).

B. Privacy Harm Insights from the United States' Sectoral Approach

The proposed regime also reflects the logical foundation — although not the implementation — of the sectoral approach to U.S. privacy law. The sectoral construction of U.S. privacy law connotes that privacy harm varies by the type and context of data disclosed.[37] Statutory penalties should similarly vary. Like the patchwork of sectoral U.S. federal privacy laws, this regime would modify damages by context. But unlike these laws, the regime would coordinate these penalties, cover the current system's many gaps in regulation, and better align the damages with the harm caused — all within an omnibus regulatory approach.

The current U.S. legal framework illustrates how the Note's regime embodies the logic of the sectoral approach that privacy harm varies by the type and context of data disclosed. Take for instance the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA punishes any covered entity that knowingly discloses another person's "individually identifiable health information."[38] HIPAA enacts a strict data security and privacy regime around protected health information, but only addresses *health* information. In the educational context, the Family Education Rights and Privacy Act of 1974 ("FERPA") restricts who may access a student's educational records and gives a student the affirmative right to access a subset of those records.[39] FERPA may truly vindicate the student's right to privacy by giving the student control over data access, not just protecting data.[40] But, the statute has limited effect beyond educational records. In a slightly different vein, the Fair Credit Reporting Act ("FCRA") regulates the access to and accuracy of "consumer reports."[41] Congress defined the term "consumer reports" broadly. FCRA therefore encompasses reports detailing a consumer's credit, "general reputation," "personal characteristics," and a host of other factors related to evaluating a consumer's credit — but not any information that does not fall within this definition.[42] In contrast to the preceding statutes which regulate specialized subject matter, the Children's Online Privacy Protection Act ("COPPA") erects privacy strictures based on the user's nature.[43] Specifically, it regulates

37. *See* Schwartz, *supra* note 6, at 325–32 (describing the sectoral and federalist aspects of U.S. privacy regulation).

38. 42 U.S.C. § 1320d-6 (2012).

39. 20 U.S.C. § 1232g (2018).

40. *Cf.* Adam D. Moore, *Intangible Property: Privacy, Power, and Information Control*, 35 AM. PHIL. Q. 365, 372 (1998) (characterizing the right to privacy as "a right to maintain a certain level of control over the inner spheres of personal information").

41. 15 U.S.C. § 1681a(d) (2018).

42. *Id.*

43. 15 U.S.C. §§ 6501–6502 (2018).

collecting and using data from children under the age of thirteen.[44] On top of these statutes, a variety of statutes regulate how the government accesses, processes, and discloses personal data.[45]

Further complicating this legal landscape, states have enacted additional sectoral privacy safeguards beyond the federal statutory floor.[46] And while some state privacy laws merely strengthen federally protected sectors, others extend to entirely new contexts. For instance, most states require that companies timely disclose a data breach to affected individuals.[47] Most states also prohibit "[i]ntentionally communicat[ing] or otherwise mak[ing] available to the general public an individual's social security number."[48] At least one court has interpreted this common statutory language to apply to data breaches. In *Curry v. Schletter, Inc.*,[49] Schletter, a manufacturer, succumbed to a "W-2 phishing email scam."[50] An unauthorized third party mimicked the digital credentials of the manufacturer and emailed a Schletter employee to request employee W-2s.[51] The employee complied.[52] This disclosure resulted in third-party access to 200 employee W-2s, which included the employees' social security numbers ("SSNs").[53] Although the Schletter employee did not intend to make the SSNs public, the court concluded that the employee intentionally sending the email brought the disclosure sufficiently within the ambit of North Carolina's SSN disclosure prohibition to survive a motion to dismiss.[54] If other courts follow this reasoning, state privacy law could more broadly regulate data breach and disclosure.

Assuming that a polity's values and preferences influence how its government legislates,[55] these statutes illustrate that the U.S. weighs certain types and contexts of information privacy more heavily than others. A sectoral approach to regulating privacy implies that the polity

---

44. *Id.*

45. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2018) (regulating information stored in federal databases); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3403 (2018) (restricting government access to consumer financial records).

46. Schwartz, *supra* note 6, at 325–27.

47. *Id.* at 327; *see generally* PHILIP ALEXANDER, DATA BREACH DISCLOSURE LAWS (2d ed. 2009).

48. N.C. GEN. STAT. ANN. § 75-62 (West 2005); *see also* 1956 R.I. GEN. LAWS ANN. § 6-48-8 (West 2008).

49. No.1:17-cv-0001-MR-DLH, 2018 WL 1472485 (W.D.N.C. Mar. 26, 2018).

50. *Id.* at *1.

51. *Id.* at *6.

52. *Id.*

53. First Amended Class Action Complaint at ¶¶ 44–45, 49, *Curry*, 2018 WL 1472485 (No.1:17-cv-0001-MR-DLH), 2017 WL 2060316.

54. *Curry*, 2018 WL 1472485, at *6–7.

55. *Cf.* Yehezkel Dror, *Values and the Law*, 17 ANTIOCH REV. 440, 440 (1957) ("[L]egal norms are closely related to various social values, being either a direct expression of them or serving them in a more indirect way."). *But see, e.g.,* Robert Tollison, *Public Choice and Legislation*, 74 VA. L. REV. 339, 341–44 (1988) (arguing that a "supply-demand process" between politicians and interest groups determines legislative outcomes).

more highly values privacy interests within the sectors regulated than outside of them. Accordingly, this relative valuation differentiates the privacy harms inhering in different sectors. This parallels the theory of privacy as "contextual integrity."[56] Helen Nissenbaum defines privacy using norms governing information flow in various social contexts.[57] Because the type of social interaction dictates what information one may appropriately disclose and how one may distribute it, breaching these norms inflicts a privacy harm.[58] Privacy harm therefore varies by the type of data unlawfully disclosed. Accordingly, a new privacy enforcement regime should vary its penalties commensurate to these differing, underlying privacy harms.

III. PROPOSING A NEW REGIME

A new regime should address both the dichotomy of inherent and attendant privacy harms — the former being best described in relation to informational autonomy or "inviolate personality," and the latter being the more concrete harms that result from a privacy violation, like economic injury — as well as the contextual variations of the inherent privacy harms. Although this Note's scope does not encompass drafting of the full statutory language or fee schedule, this Part overviews the proposed enforcement regime. The first Section details the elements of the regime itself. The second Section then explores the practical benefits of implementing the regime and argues why industry and consumers might support it.

A. The Regime Itself

The regime should bifurcate enforcement by (1) empowering the Federal Trade Commission ("FTC") to seek statutory damages for inherent privacy harms[59] and (2) allowing private individuals to seek attendant damages. After obtaining statutory damages for an unlawful

56. Nissenbaum, *supra* note 13, at 136.

57. *Id.* at 137.

58. *Id.* at 138–45.

59. The preemptive federal enforcement fits best under the mantle of the FTC's consumer protection mission. Although Congress could entrust enforcement to a new privacy-focused body, the FTC already acts as the U.S.'s de facto data protection authority. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–606 (2014). And despite the FTC's privacy jurisdiction only manifesting with unfair or deceptive trade practices, *see* LabMD v. Fed. Trade Comm'n, 894 F.3d 1221, 1224 (11th Cir. 2018) (vacating an FTC order to overhaul an inadequate data security program for falling outside of its jurisdiction), the FTC views itself as the "nation's primary privacy and data security enforcer." Press Release, FTC, FTC Releases 2018 Privacy and Data Security Update (Mar. 15, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-privacy-data-security-update [https://perma.cc/P2RB-GCKE]. In 2018 alone,

data disclosure, the FTC would then distribute them to the victims of the disclosure. This centralized remedial mechanism would obviate the need for most private class-action suits. One could litigate privately *only* to recover actual, attendant damages flowing from unlawful disclosure of one's data. This regime also slots into other potential data security regimes. For instance, Congress could adopt a reasonable data security standard that creates a safe harbor from this penalty schedule.[60] Or Congress could employ this regime to incentivize data brokers to act as "information fiduciaries."[61] Under this option, a firm that voluntarily adopted the information fiduciary model could escape, or mitigate, the regime's penalties.[62] Finally, this regime could stand alone and incorporate either a negligence or strict liability standard.

Substantive rules aside, the new statutory regime would also preempt state law. Although state laws merely prohibit eschewing or delaying notice to breach victims [63] and intentionally publicizing SSNs,[64] preemption could invalidate elements of future state regulation. The CCPA illustrates this issue. It bestows a private right of action upon any individual who suffers "unauthorized access and exfiltration, theft, or disclosure" of their data if it stemmed from a business lacking "reasonable security procedures."[65] Private litigants seeking state law statutory damages for the same inherent privacy harms subject to federal enforcement would needlessly complicate the system, doubly punish companies in California (and any other states adopting CCPA analogs), and increase litigation transaction costs.

This preemption would narrow the scope of private suits. That is, it would preclude privately litigating a claim if it encroached on the regime. But the proposal would still allow privately seeking damages for injuries not inherent to privacy harm. Privacy injuries extending beyond a data breach's inherent privacy harm would survive. For instance, if a party disseminated sensitive information that caused a reputational harm, the victim could sue for public disclosure of private

---

the FTC dismantled a revenge porn website, settled enforcement actions over privacy violations with Venmo and Uber, and enforced a three-million-dollar Fair Credit Reporting Act penalty against RealPage Inc. *Id.*

60. *Cf.* Patricia Cave, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 790–91 (2013) (arguing that new legislation should authorize the FTC to set minimum data security standards and penalize noncompliance).

61. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C.D. L. REV. 1183, 1221–29 (2016) (arguing that the law should create or encourage a fiduciary relationship between a company possessing consumer data and that consumer). Under this regime, a firm that adopted the information fiduciary model could escape or mitigate punishment. *Id.*

62. *See id.* at 1229 (noting that safe harbors could encourage adopting the information fiduciary model).

63. *E.g.*, WASH. REV. CODE ANN. § 19.255.010 (West 2019).

64. *E.g.*, N.J. STAT. ANN. § 56:8-164 (West 2019).

65. The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150(a)(1) (West 2019).

facts.[66] Additionally, if the party distorted the information, the victim could sue for defamation.[67] And if a breach clearly resulted in economic harm via identity theft, the resulting private action would survive preemption. Under the model, a private action that did not reference an inherent privacy harm would fail.

The proposed penalty scheme of the regime's government enforcement is more precise than the flat fines or discretionary ranges common to most statutory damages. For example, the CCPA establishes a statutory penalty of up to "seven thousand five hundred dollars ($7,500) for each intentional violation" but does not provide any criteria for setting individual penalties.[68] In contrast, the regime would employ a fee schedule coupled with context-based modifiers. This aligns the statutory damages with the actual, inherent privacy injury that a victim of an unlawful data disclosure experiences.[69]

First, the regime assigns different statutory penalties to different types of data. Just as the privacy harm of disclosing one's SSN or medical conditions likely eclipses that of disseminating one's online shopping history, so too would the regime penalize disclosing the former data more severely than disclosing the latter. This categorization of penalties into tiers also aligns the system with how technology firms monetize data. Data brokers aggregate different types of data into packages to be sold at different prices.[70] Analogously pricing the penalties for disclosing this data therefore imposes a fitting, proportionate justice.

Second, the regime modifies the penalty in certain data contexts. This transformation better maps the statutory penalties to the actual privacy harm that the disclosure inflicts. For instance, taking into account the importance of children's privacy as illustrated by COPPA, the regime could increase the penalty associated with a parent's breached data if the breach also included information about their child. If disclosing a parent's information makes their child's data more identifiable and more manipulatable, the privacy harm inflicted upon both the parent and child might exceed the sum of the individual privacy harm's parts. These modifiers could extend beyond the obvious health, educa-

66. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 392–98 (1960) (describing the use and limitation of tort law to protect from the privacy harm stemming from the public disclosure of private facts).

67. *Cf.* Solove, *supra* note 10, at 549–50 (linking the defamation cause of action to reputational harms flowing from distorting private information).

68. The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.155(b) (West 2019).

69. *See supra* Part II.

70. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 19–20 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/5DLL-XLW4].

tion, family, and financial contexts. Third parties can abstract new, sensitive, and seemingly-unrelated information from existing personal data via profiling.[71] These techniques potentiate a disclosure's privacy harm far beyond the sum of the harm of disclosing the independent data separately. Take the popularly reported story in which Target's data profiling programs predicted a high school student's pregnancy before she had informed her father.[72] Using only the student's buying habits and a statistical analysis of previous shoppers, Target predicted the student's pregnancy.[73] The media focused on the power of corporate commercial profiling and the story's personal aspects: Target mails baby-related coupons to a high school student.[74] The father angrily confronts a store manager over sending these coupons to his ostensibly non-pregnant daughter.[75] The daughter reveals her pregnancy to her father.[76] The father sheepishly apologizes to Target.[77] But this scenario illuminates a data breach's more nuanced risk. By applying machine learning and statistical methods to seemingly innocuous but illicitly obtained data, bad actors could extrapolate far more sensitive and damaging information.[78] The regime's contextual modifiers would therefore incorporate profiling's transformative effect when increasing fines for disclosing combinations of certain data. Although an exhaustive list of contextual modifiers exceeds the scope of this Note, potential modifiers include:

(1) The data's informational context (e.g., healthcare, credit reporting);

(2) The amount of data disclosed (if the disclosure's harm increases cumulatively or exponentially);

(3) The identity of the party who now possesses the information (if known);[79]

(4) The remedial measures taken by the culpable party (if any);

---

71. *See* Francesca Bosco et al., *Profiling Technologies and Fundamental Rights: An Introduction*, in PROFILING TECHNOLOGIES IN PRACTICE 5, 13 (Niklas Creemers et al. eds., 2015) (arguing that profiling can synthesize sensitive data about an individual from combinations of anonymized data).

72. Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [https://perma.cc/P9KK-S9TP].

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

78. *See* Bosco et al., *supra* note 71, at 13.

79. Beyond just the potential for economic harm, this factor reflects by what degree the disclosure violates norms of distribution. *See* Nissenbaum, *supra* note 13, at 140–43.

(5) The affected party's explicit consent or nonconsent to their data processing;

(6) The degree of the data's anonymity; and

(7) The presence of safeguards against reidentification.[80]

By assigning penalties to discrete data types and modifying them in different contexts, this system expands upon the explicit and implicit data breach tiers found in current laws. For example, HIPAA's unlawful disclosure penalties vary according to a violator's culpability and actions.[81] And, by regulating privacy sectorally, the U.S. regime implicitly assigns different penalties for disclosing different types of data in different contexts.[82] Finally, beyond these civil penalty analogs, remunerative frameworks — particularly physician fee schedules — inform the proposal. The MPFS assigns maximum prices (i.e., reimbursement limits) to discrete medical services.[83] Then, depending on the presence of certain contextual factors or circumstances, it applies modifiers. For instance, if a physician performs a surgery bilaterally,[84] she applies modifier 50.[85] This modifier increases the performed surgery's price by 150%, which reflects the increased cost and effort of a bilateral procedure.[86] But if a surgical assistant performed a certain procedure, she would apply modifier 80, which reduces the procedure's price by eighty-four percent.[87] This incorporates the lower relative cost of an assistant.[88] By applying these modifiers to the fee schedule, the MPFS harmonizes physician reimbursement with a procedure's cost and value. The proposed regime parallels the MPFS's attempt at greater monetary precision. It just does so punitively.

---

80. For example, employing differential privacy methods. *See generally* Kobbi Nissim et al., *Bridging the Gap Between Computer Science and Legal Approaches to Privacy*, 31 HARV. J.L. & TECH. 687, 714–18 (2018).

81. *See* 45 C.F.R. § 160.404 (2016) (establishing penalty tiers for HIPAA data violations).

82. But the current U.S. regime fails both in its breadth and its depth: Federal law only covers a few key sectors while leaving most consumer data unregulated. And these sectoral laws fail to capture the complexity of different data's potential privacy harm and adequately compensate victims from unlawful disclosure. *See supra* Section II.B.

83. *See* 83 Fed. Reg. 59,453 (Nov. 23, 2018) (revising the MPFS).

84. On a patient's right and left sides, which requires "separate sterile fields and a separate surgical incision." CARESOURCE, SUBJECT: BILATERAL PROCEDURES 1 (2013), https://www.caresource.com/documents/bilateral-procedures [https://perma.cc/967Y-9XAN].

85. 83 Fed. Reg. 59,461 tbl.3 (Nov. 23, 2018).

86. *See id.*

87. *See id.*; *see also Modifier 80*, NORIDIAN, https://med.noridianmedicare.com/web/jeb/topics/modifiers/80 [https://perma.cc/4U48-9VH9].

88. *Compare* Beth Greenwood, *Surgical Assistant Vs. Surgical Technologist*, CHRON, https://work.chron.com/surgical-assistant-vs-surgical-technologist-15223.html [https://perma.cc/MD8K-Y5N5] (listing the average 2016 salaries for surgical assistants at $101,480 and surgical technologists at $45,160), *with Surgeon Salary in the United States*, SALARY.COM, https://www1.salary.com/Surgeon-Salary.html [https://perma.cc/W2Q5-NSDW] (estimating the average 2019 U.S. surgeon salary at $387,733).

B. Why Industry and Consumers Might Accept the Regime

Businesses and consumers would likely, and loudly, object to this regime — at least initially. Businesses might balk at the regime's punitive nature. Consumers might lament losing their private right of action — and through it, their autonomy. But this regime benefits both data-storing businesses and consumers. This Section details the elements of the regime that might induce industry and consumers to support it: state law preemption, reduced private litigation (and corresponding costs), and better vindication of consumer rights.

1. State Law Preemption

First, the regime preempts state law to create one national privacy regime. To industry's dismay, the patchwork of state privacy regulations complicates compliance[89] and allows states to regulate more aggressively than they would under a national regime. For example, the CCPA, although arguably less aggressive than the GDPR,[90] regulates and penalizes data processors far more aggressively than many federal proposals.[91] As compared to other more prescriptive federal regimes, this proposal would satisfy industry's stated interests in preemption and consistency.[92]

2. Reduced Private Litigation and Transaction Costs

Second, by limiting private suits to direct economic harms — i.e. attendant harms — flowing from the disclosure the regime would

89. Daniel Castro & Alan McQuinn, *Opinion: Why We Need a Robust National Standard for Breach Notification*, CHRISTIAN SCI. MONITOR (June 10, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0610/Opinion-Why-we-need-a-robust-national-standard-for-data-breach-notification [https://perma.cc/E7EP-3VBJ] (noting the difficulty of complying with the forty-eight different jurisdictions' data breach notification laws).

90. *See Your Readiness Roadmap for the California Consumer Privacy Act (CCPA)*, PWC, https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html [https://perma.cc/2QH5-6UXR].

91. *Compare* The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 *et seq.* (West 2019), *with* ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA app. 63–64 (2019) (proposing data privacy legislation recommendations that reflect compromises between privacy and innovation interests), *and* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 35–39 (2012) (proposing a stakeholder-driven consumer privacy bill of rights with a safe harbor more expansive than the CCPA's).

92. *See, e.g.*, *What Are the Elements of Sound Data Breach Legislation?: Hearing Before the Subcomm. on Commerce Mfg. & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 12–14, 20–21, 26–28, 34, 40 (2015) [hereinafter *Data Breach Legislation Hearing*] (detailing various industry representatives requesting preemption and nationally consistent data privacy regulation).

lessen the frequency of private litigation. This diminution would reduce industry's litigation and legal transaction costs.[93] Industry has unsuccessfully lobbied Congress to eliminate the private right altogether, so a centralized enforcement regime with a substantially reduced private right might prove an acceptable compromise.[94] The regime would occupy a middle-ground between omnibus privacy regimes (like the CCPA and GDPR) and many federal sectoral privacy statutes. The former confers expansive private rights of action to data subject; the latter often does not confer private rights at all.[95] This litigative compromise would satisfy many industry preferences while still deterring and compensating for privacy harms. And businesses could more easily predict their data breach liability as well. By applying the penalty fee schedule to its existing trove of consumer data, a data processor could easily calculate its total data breach liability — before a breach even occurs. Computing enforcement liability ex ante allows businesses to price privacy into their services or insure against privacy risk.[96] This ex ante approach would benefit both government and industry. For instance, economic research shows that ex ante regulation, like corrective taxes, often induces myopic producers to invest optimally.[97] Somewhat analogously, Miriam Baer argues that levying a corrective tax on police violating the Fourth Amendment incentivizes police to engage in less risky behavior and alleviate constitutional issues.[98] She proposes a fee schedule that assigns a price to each violation relative to its risk.[99] Here, the regime proposed in this Note provides comparable ex ante regulation that, if priced correctly, would induce data security measures congruent with the full impact of a data breach, rather than merely the variable, remote costs of settling a class action.[100]

Commentators have argued that major privacy violators, like Facebook, merely incorporate privacy fines into the cost of their service

---

93. *See* MCQUINN & CASTRO, *supra* note 91, at 61.

94. *See, e.g.*, *Data Breach Legislation Hearing*, *supra* note 92, at 35 (requesting, on behalf of Retail Industry Leaders Association, that Congress not authorize any private right of action in any potential civil data breach penalty legislation); *id.* at 39–40 (requesting the same on behalf of data processing firm Acxiom); *id.* at 30 (requesting, on behalf of 2,200 technology firms, that Congress ban private rights of action for data breach notification laws).

95. *See* MCQUINN & CASTRO, *supra* note 91, at 61.

96. *See generally* David J. Baldwin et al., *Insuring Against Privacy Claims Following a Data Breach*, 122 PENN. ST. L. REV. 683 (2018) (discussing the market for cyber and data breach insurance policies).

97. Brian Galle, *In Praise of Ex Ante Regulation*, 68 VAND. L. REV. 1715, 1734–38, 1749–52 (2015).

98. Miriam H. Baer, *Pricing the Fourth Amendment*, 58 WM. & MARY L. REV. 1103, 1108–10 (2017).

99. *Id.* at 1139.

100. *Cf.* Galle, *supra* note 97. Even if ex ante liability would not placate overregulation concerns, Congress could tailor the onus of substantive data security, liability, or fiduciary standards accordingly. This Note's regime forms only a piece of the regulatory puzzle. Other mitigating prescriptive measures could offset the regime's punitive nature.

without improving consumer privacy protections.[101] That major privacy violators might see these fines as a cost of doing business does not vitiate this regime. First, this argument partially clashes with economic theory: Facebook, as a monopolist,[102] will set its prices at the optimal profit-seeking level, so accounting for these fines would substantially reduce data sales.[103] Second, higher fines — ones much higher than the cost of adopting good data policies — might deter these companies' violative conduct.[104] Congress, or the FTC, could simply set this regime's penalties at levels sufficient to deter bad behavior — including modifying the penalty based on the culpable party's revenue.[105] Third, the regime's focus on enforcement allows it to slot into a more substantive data security and privacy framework.[106] If this regime alone fails to induce better data privacy practices, Congress could couple the regime with substantive data privacy practices or criminal penalties. Finally, inducing better practices among data monopolists, like Facebook and Google, may also require antitrust solutions beyond the scope of this Note.[107]

---

101. *E.g.*, Sarah Miller & David Segal, *Break Up Facebook: Latest Hack Proves It's a Dangerous Monopoly That a Fine Won't Fix*, USA TODAY (Oct. 5, 2018, 12:55 PM), https://www.usatoday.com/story/opinion/2018/10/05/facebook-dangerous-monopoly-divest-instagram-whatsapp-messenger-column/1512215002 [https://perma.cc/RR8H-SVST].

102. *See* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 81–90 (2019) (describing Facebook's monopolistic position, including controlling over eighty percent of consumer time on social media); David McLaughlin, *Are Facebook and Google the New Monopolies?: QuickTake Q&A*, BLOOMBERG (July 13, 2017) https://www.bloomberg.com/news/articles/2017-07-13/antitrust-built-for-rockefeller-baffled-by-bezos-quicktake-q-a [https://perma.cc/6UZT-EMZA] (noting that, as of 2017, Facebook and Google control about fifty-six percent of the U.S. market for mobile advertising).

103. *See* Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499, 524–25 (1961) (arguing the same but with respect to tort damages).

104. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, *in* ESSAYS IN THE ECONOMICS OF CRIME AND PUNISHMENT 1, 17 (1974)*;* Troy Wolverton, *The FTC's $5 Billion Fine for Facebook Is So Meaningless, It Will Likely Leave Zuckerberg Wondering What He Can't Get Away With*, BUS. INSIDER (July 12, 2019, 07:35 PM) https://www.businessinsider.com/facebook-5-billion-ftc-fine-a-slap-on-the-wrist-2019-7 [https://perma.cc/PP86-8PPA] (sharing the view of many commentators that FTC's five-billion-dollar settlement with Facebook amounted to "a slap on the wrist").

105. *See* Becker, *supra* note 104, at 30 n.46 (citing Jeremy Bentham as a proponent of adjusting penalties relative to the offender's wealth).

106. *See supra* notes 60–62 and accompanying text.

107. *See* Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources: Background Information on the Bundeskartellamt's Facebook Proceeding (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html [https://perma.cc/G4ES-GTLJ] (describing the data reforms the German competition authority mandated Facebook implement); Srinivasan, *supra* note 102, at 98–99 (arguing that remedying Facebook's data privacy issues requires addressing Facebook's monopoly position and anticompetitive behavior).

3. Better Vindication of Consumer Rights

Unconvinced by the regime centrally enforcing their rights, consumers might object that the narrowed private right of action unfairly diminishes their autonomy. But this objection presupposes that private data breach litigation actually remedies privacy harms, compensates victims, and validates consumer autonomy. Currently, circuit splits and uncertain outcomes hinder the industry from calculating costs and therefore investing in data security.[108] And as Eric Goldman notes, class action suits often enrich the plaintiffs' bar and class representatives, but deprive the remaining plaintiffs of compensation.[109] This compensatory failing aside, Goldman argues, privacy class action suits fail to validate plaintiffs' autonomy.[110] The control and choice of how a suit proceeds often lies overwhelmingly with the lawyers.[111] Despite autonomy dominating privacy theory, privacy class actions may not actually enhance consumer autonomy. Although the Note's regime also deprives data breach victims of direct control, it at least empowers the FTC — ostensibly an agency democratically accountable to victims — to obtain meaningful compensation for victims and vindicate their rights.[112] And by associating specific costs with unlawfully disclosing data, the proposed regime should induce cost-effective data security measures commensurate with the expected value of a breach's penalties.[113] Consumers may therefore accept a nominal autonomy loss for a real improvement in outcomes.[114]

---

108. *See* Kristen L. Burge, *Your Data Was Stolen, But Not Your Identity (Yet)*, AM. BAR ASS'N (Jan. 11, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/your-data-was-stolen-not-your-identity-yet [https://perma.cc/SS9Z-VM9J] (describing the circuit split over standing in data breach suits); Goldman, *supra* note 8, at 318, 318 n.47 (arguing that privacy class action suits frequently fail and listing demonstrative cases).

109. Goldman, *supra* note 8, at 314–16 (citing privacy class action suits that directed millions of dollars to the plaintiffs' attorneys but nothing to non-representative plaintiffs).

110. *Id.* at 310–14.

111. *Id.*

112. The "overwhelming" public response to the $125 in restitution that consumers could claim through the Equifax settlement — without showing economic injury — evidences potential consumer support for this Note's regime. *See* Kate Fazzini, *Equifax Might Run Out of Settlement Cash, FTC Warns*, NBC NEWS (July 31, 2019, 03:35 PM), https://www.nbcnews.com/tech/security/equifax-might-run-out-settlement-cash-ftc-warns-n1037371 [https://perma.cc/8VBE-5VLY]. But the regime would set penalties and recovery so all affected consumers could collect — not just the first to file. *See id.*

113. *See, e.g.*, William M. Landes & Richard A. Posner, *The Positive Economic Theory of Tort Law*, 15 GA. L. REV. 851, 868–72 (1980) (arguing that parties invest in "due care" until their prevention costs equal a tort suit's expected loss).

114. These outcomes and the regime may also benefit consumer privacy architecturally — i.e. systemic privacy issues embedded in the social and legal ecosystem. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 99–101 (1972). By showcasing the government vindicating individual privacy rights and deterring unlawful disclosure, this regime might enhance individual privacy, consumer perception of privacy, and government legitimacy. *See id.*

IV. CONCLUSION

Disclosing private data inflicts two distinct classes of injury: inherent privacy harm and attendant privacy harm flowing from violating one's privacy. Within the former, the type and context of data disclosed dictate the harm's severity. Privacy legislation should address these nuances of privacy harm. This Note proposes a bifurcated enforcement regime that does just that. It suggests that Congress empower the FTC to enforce statutory privacy penalties that reflect the type of data that is unlawfully disclosed and the context of its disclosure. This penalty and modifier schedule would parallel the MPFS. The government would then distribute the proceeds to a disclosure's victims. The regime would then narrow a consumer's right of private action to encompass injuries flowing from violating one's privacy. Once incorporated into a prescriptive framework, this regime would tailor punishment and victim compensation to the actual harm of violating one's privacy.