Boston College Law Review

Volume 60 | Issue 7 Article 3

10-30-2019

A Private Enforcement Remedy for Information Misuse

Peter C. Ormerod
Western Carolina University, pcormerod@wcu.edu

A PRIVATE ENFORCEMENT REMEDY FOR INFORMATION MISUSE

PETER C. ORMEROD

A PRIVATE ENFORCEMENT REMEDY FOR INFORMATION MISUSE

PETER C. ORMEROD*

Abstract: Misuse of users' personally identifiable information is persistent and pervasive. This Article addresses two questions: why is information misuse so common and so severe and how could domestic law change to make it less so? I use a simple model to illustrate that companies externalize information misuse costs onto users, which has two related but distinct effects: chronic underinvestment in information security and excessive retention of user data. I then seize on this observation to propose a specific legal vehicle at the heart of this Article—a private enforcement remedy. This private enforcement remedy has four essential features. First, the remedy must be created under state law. State law provides a viable alternative when federal courts have used the constitutional standing doctrine to express overt hostility to privacy harms. Second, the law should impose a fiduciary duty on entities that collect or retain users' information. Structuring the remedy this way insulates it from attack by a weaponized First Amendment. Third, breach of an information fiduciary's duty should be a strict liability tort. The arguments for strict liability in products liability cases apply with even greater force to informational harms. Fourth, the statute that creates this private enforcement remedy should prescribe a schedule that begins with nominal damages and attorney's fees for strict liability, and it should increase monetary penalties with a defendant's culpability. The remedy's central purpose is to reshape incentives, so the damages schedule should not be unduly punitive or effect a windfall for plaintiffs' attorneys.

INTRODUCTION

If you are an American with a credit card, your identity was almost certainly stolen in 2017.[1] If you ever had a Yahoo account, at least one hacker group—and perhaps more—walked off with the keys to your account a few

* Assistant Professor of Business Law, Western Carolina University. Thanks to the participants in the 2019 Huber Hurst Research Seminar at the University of Florida's Warrington College of Business. Thanks also to Ivy Gibson and Kenneth Sanney for providing feedback on an earlier draft.

[1] *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/JN6Z-XCZA] ("If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax . . . .").

years earlier.[2] Even if you never had an account with Facebook or Instagram, Facebook knows who you are, maintains a secret dossier about you, and provides that dossier to advertisers—but you can neither access nor delete that information.[3]

The devices in your home are listening to you and sometimes send recordings of your conversations to your acquaintances.[4] Your wireless service provider knows every single place you go and—until recently—gave that information to law enforcement when it asked.[5] Ninety-two percent of the websites you visit have embedded Google trackers, so Google knows just about every place you visit on the Internet—whether or not you have a Google account or use any Google services.[6] There were over three billion unique and real identities exposed online in 2017, which represents a sixty-four percent increase over 2016.[7]

---

[2] *See* Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/3FLB-WFLK] ("Digital thieves made off with names, birth dates, phone numbers and passwords of users that were encrypted with security that was easy to crack. The intruders also obtained the security questions and backup email addresses used to reset lost passwords . . . .").

[3] *See* Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information*, GIZMODO (Sept. 26, 2018), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051 [https://perma.cc/W7TM-4X9D]; Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met*, GIZMODO (Nov. 7, 2017), https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691 [https://perma.cc/VNT3-VJN6].

[4] *See* Heather Kelly, *How an Alexa Speaker Recorded and Shared a Private Conversation*, CNN (May 24, 2018), http://money.cnn.com/2018/05/24/technology/alexa-secret-recording/index.html [https://perma.cc/2L2Q-W3G4]; *see also* Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/B84A-89JV]; Alex Hern, *Apple Contractors 'Regularly Hear Confidential Details' on Siri Recordings*, THE GUARDIAN (July 26, 2019), https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings [https://perma.cc/D64S-GMN8]; James Vlahos, *Smart Talking: Are Our Devices Threatening Our Privacy?*, THE GUARDIAN (Mar. 26, 2019), https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy [https://perma.cc/W89J-R9BD].

[5] *See, e.g.*, *AT&T February 2017 Transparency Report* 4 (Feb. 10, 2017), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf [https://perma.cc/4YYX-LL24] (reporting that the company received 50,000 requests for customers' location history from law enforcement in 2016). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (holding that the warrantless acquisition of cell-site location information violated the Fourth Amendment).

[6] Ibrahim Altaweel et al., *Web Privacy Census*, TECH. SCI. (Dec. 15, 2015), https://techscience.org/a/2015121502/ [https://perma.cc/2PKG-6XAF] ("We found that Google tracking infrastructure is on 92 of the top 100 most popular websites and on 923 of the top 1,000 websites, providing Google with a significant surveillance infrastructure online.").

[7] *See 2018 4iQ Identity Breach Report* 5 (May 2018), https://webcdn.4iq.com/2019/05/10191838/2018_IdentityBreachReport_4iQ.pdf [https://perma.cc/JQ9H-2URT].

These examples and more demonstrate that the excessive collection, retention, and misuse of users' personally identifiable information is both persistent and pervasive. This Article addresses two questions: why does information misuse keep happening and what, if anything, can we do to make information misuse less frequent and less severe?

Many people would probably feel uncomfortable entrusting their physical belongings to a company that cannot be held liable for misusing those things. Yet this basically describes the current information security regulatory environment. A brief review of authorities reveals that there is no meaningful legal deterrent for information misuse. By and large, the authorities that do exist are grossly inadequate and that is only starting to change at the margins. I explain that there is no legal mechanism for punishing or deterring information misuse and illustrate that preventing information misuse is often an irrational decision.

If we agree that providing users with a new remedy would help reshape incentives, what would that remedy need to look like? The heart of this Article is a specific policy proposal, which I refer to as a private enforcement remedy. To be effective, this remedy must have four features.

First, the remedy must be created under state law. In recent years, the federal courts, led by the Supreme Court, have made it increasingly difficult to vindicate information security rights and harms under the doctrine of constitutional standing. At the Supreme Court, this trend most recently culminated in the 2016 decision *Spokeo v. Robins*, which held that a statutorily recognized right was not sufficiently "concrete" under Article III to constitute a "case or controversy" that could be adjudicated by federal courts.[8] *Spokeo* and its progeny in the lower courts are an enormous problem for information security regulatory reform because users whose information has been compromised are generally foreclosed from suing in federal court. Thankfully, Article III's demanding injury-in-fact requirement applies only in federal court. The states are free—indeed, I argue, designed and assumed—to provide a forum for wide-ranging relief from harms that are (arguably) insufficiently concrete in federal court. Below, I trace the origins of constitutional standing, explain *Spokeo*, and summarize a host of post-*Spokeo* digital privacy standing cases. These threads culminate in my contention that the private enforcement mechanism must be created under state law.

Second, the remedy must impose a fiduciary duty on entities that collect or retain personally identifiable information. Scholars have begun refining a framework for resolving information-related harms that minimizes potential

[8] *See* Spokeo v. Robins, 136 S. Ct. 1540, 1550 (2016).

First Amendment hurdles.[9] This framework establishes a fiduciary relationship between users and the businesses that collect and retain their personally identifiable information. Below, I build on this work, arguing that states should enact legislation that would codify a tort for the breach of an information fiduciary's duty. This avenue is both good policy and sound strategy because it minimizes First Amendment arguments against vindicating informational harms.

Third, defendants should be strictly liable for information misuse. Strict liability is appropriate when two conditions are met: First, strict liability is necessary when there is significant difficulty attributing liability under a standard negligence regime. This is true in the products liability context—successfully establishing duty, breach, and cause is extremely difficult in the complex supply-chain environment of the modern economy. Second, strict liability is appropriate when the defendant is better able to discover the danger and has a superior ability to bear the costs of injury. This is also true in the products liability context, where the law holds manufacturers strictly liable because they are far better positioned to avoid and shoulder the cost of the harm. Below, I argue that information misuse satisfies both of these conditions, and I build on other scholars' work in this area to establish that breach of an information fiduciary's duty should be treated as a strict liability tort.

Fourth, the statute should prescribe a schedule of damages that begins with nominal damages and attorney's fees for strict liability and ratchets up damages with a defendant's culpability. Appropriately deployed, this so-called private attorney general regime can be a powerful force that reshapes incentives. I argue below that private enforcement is particularly well-suited for information misuse. At the same time, the law should not effect a windfall for plaintiffs' attorneys when tangible harm may be difficult to prove.

In this Article I describe the reasons for each of these features in greater detail and then consider the benefits and drawbacks of this approach. These benefits include practical and logistical advantages and would also further three primary ends. First, this scheme will reshape incentives by internalizing the costs of information misuse. Second, this mechanism will, for the first

---

[9] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON 102–03 (2004) ("I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us."); ARI EZRA WALDMAN, PRIVACY AS TRUST 47 (2018) ("[T]he law of information privacy should be oriented toward buttressing . . . trust norms . . . when those with power (information holders) violate the trust of those without (information sharers)."); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1210 (2016) ("Generally speaking, when the law prevents a fiduciary from disclosing or selling information about a client—or using information to a client's disadvantage—this does not violate the First Amendment, even though the activity would be protected if there were no fiduciary relationship.").

time, impose some substantial costs for excessive information retention. I argue that this is an unbridled benefit, and it is a goal that has been neglected in both scholarly and policy debates. Third, structuring the remedy this way will benefit the cybersecurity insurance market, thereby helping disperse information misuse costs in a more just and equitable way.

When I use the terms "information misuse" and "data misuse," I am using them expansively and to encompass at least four distinct things. First is data breaches by external actors. These include cases where users' information is compromised by a nefarious actor outside the organization.[10] Second is when an external actor misuses information. This includes the Cambridge Analytica scandal, where a Facebook app developer breached Facebook's terms of service when he—under the auspices of academic research—collected users' data and provided that trove of information to a for-profit political consulting firm.[11] Third is when internal actors misuse information. This includes examples where employees use their privileges to exploit users' information for illegitimate purposes that are unrelated to the business—such as Uber's "God View" and Facebook's termination of an employee who used his position to stalk women.[12] And fourth is when the company itself uses data for an illegitimate purpose. This includes, for example, Facebook's practice of providing advertisers with users' cell phone numbers, even when the company only acquired those numbers for multifactor authentication purposes.[13] This fourth

---

[10] *Glossary*, NICCS, https://niccs.us-cert.gov/glossary [https://perma.cc/98BV-624Y] (defining data breach as "[t]he unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information"); *id.* (defining data theft as "[t]he deliberate or intentional act of stealing of information").

[11] *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/XJ4V-7LE5].

[12] *See, e.g.*, Joseph Cox, *Facebook Is Investigating a Claim That an Employee Used His Position to Stalk Women*, VICE: MOTHERBOARD (Apr. 30, 2018), https://motherboard.vice.com/en_us/article/kzxdny/facebook-investigating-employee-stalking-women-online [https://perma.cc/4J78-B36E]; Kashmir Hill, *'God View': Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure*, FORBES (Oct. 3, 2014), https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/ [https://perma.cc/KL8U-ZNZG]; Sam Levin, *Facebook Fires Engineer Accused of Stalking, Possibly by Abusing Data Access*, THE GUARDIAN (May 2, 2018), https://www.theguardian.com/technology/2018/may/02/facebook-engineer-fired-alleged-stalker-tinder [https://perma.cc/8A99-9WXJ].

[13] *See* Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information*, *supra* note 3; Giridhari Venkatadri et al., *Investigating Sources of PII Used in Facebook's Targeted Advertising*, PROCEEDINGS ON PRIVACY ENHANCING TECHS. (2019), https://mislove.org/publications/PII-PETS.pdf [https://perma.cc/HG9J-LVCM].

category also encompasses slightly different examples, such as when a company misrepresents to users (and regulators) that it's protecting information more robustly than it actually is.[14]

Part I of this Article summarizes the current information security regulatory environment.[15] Part II explains that information misuse is a market failure.[16] Part III proposes a solution for this market failure: create a state-law cause of action for breach of an information fiduciary's duty, impose nominal damages for strict liability, and ratchet up damages with culpability.[17] Part IV justifies each component of this proposal by explaining the rationale for using state law, for creating a fiduciary duty, for imposing strict liability, and for levying nominal damages.[18] Part V examines the advantages of and challenges to this remedial scheme.[19]

I. THE CURRENT INFORMATION SECURITY REGULATORY ENVIRONMENT

Information security regulation in the United States is composed of a complicated patchwork of authorities. The following Sections in this Part will provide overviews of different regulatory regimes.[20] Section A of this Part provides a brief overview of federal law authorities.[21] Section B focuses on state law authorities.[22] Section C offers an overview of foreign law authorities.[23]

A. Federal Law

There are many federal statutes that regulate information security in a limited way. I list a few of these sector-specific statutes first and then turn my attention to two slightly more robust regulators: the Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC).

---

[14] *See, e.g.*, Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. TIMES (June 3, 2018), https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html [https://perma.cc/NN6V-E9VD] ("But the partnerships [between Facebook and device manufacturers] . . . raise concerns about the company's privacy protections and compliance with a 2011 consent decree with the Federal Trade Commission. Facebook allowed the device companies access to the data of users' friends without their explicit consent, even after declaring that it would no longer share such information with outsiders. Some device makers could retrieve personal information even from users' friends who believed they had barred any sharing, The New York Times found.").

[15] *See infra* notes 23–118 and accompanying text.

[16] *See infra* notes 120–138 and accompanying text.

[17] *See infra* notes 141–155 and accompanying text.

[18] *See infra* notes 160–318 and accompanying text.

[19] *See infra* notes 323–348 and accompanying text.

[20] This overview is not comprehensive and exhaustive, but it hits the high points.

[21] *See infra* notes 24–63 and accompanying text.

[22] *See infra* notes 64–102 and accompanying text.

[23] *See infra* notes 103–118 and accompanying text.

1. Sector-Specific Federal Statutes

Over time, Congress has enacted several statutes that regulate specific sectors' information security practices. These include:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (regulating healthcare information);[24]
- Financial Services Modernization Act of 1999, a.k.a. Gramm-Leach-Bliley Act (GLBA) (regulating financial sector information);[25]
- Fair Credit Reporting Act (FCRA)[26] and Federal Accurate Credit Transactions Act (FACTA) (regulating consumer credit reporting information);[27]
- Privacy Act of 1974 (regulating government record retention practices);[28]
- Children's Online Privacy Protection Act (COPPA) (regulating internet-collected information about children);[29]
- Family Educational Rights and Privacy Act of 1974 (regulating education records);[30] and
- Electronic Communications Privacy Act of 1986 (regulating electronic communications and law enforcement).[31]

Excluded from this list but detailed below are consumer protection regulations by the FTC and investor protection regulations by the SEC.

---

[24] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[25] Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999 (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 and 15 U.S.C.). In 2019, the FTC proposed significant amendments to two of GLBA's privacy-related implementing regulations: the Privacy Rule and the Safeguards Rule. *See Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act*, 84 Fed. Reg. 13,150 (proposed Apr. 4, 2019), https://www.federalregister.gov/documents/2019/04/04/2019-06039/privacy-of-consumer-financial-information-rule-under-the-gramm-leach-bliley-act [https://perma.cc/G5CD-8WFC] (Privacy Rule); *Standards for Safeguarding Customer Information*, 84 Fed. Reg. 13,158 (proposed Apr. 4, 2019), https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information [https://perma.cc/2F66-HJXD] (Safeguards Rule).

[26] Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, 84 Stat. 1127 (codified as amended in 12 and 15 U.S.C.).

[27] Federal Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in 15 U.S.C.).

[28] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[29] Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended at 15 U.S.C. §§ 6501–6506).

[30] Family Educational Rights and Privacy Act of 1974, Pub. L. No. 90-247, 88 Stat. 571 (codified as amended at 20 U.S.C. § 1231).

[31] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended throughout 18 U.S.C.).

2. FTC Enforcement

Section 5 of the Federal Trade Commission Act outlaws "unfair or deceptive acts or practices in or affecting commerce"[32] and "empower[s] and direct[s]" the FTC to prevent persons and businesses from using deceptive and unfair trade practices.[33]

Courts have given this simple prohibition an expansive interpretation, providing the FTC with a broad mandate to pursue companies that fail to adequately protect users' and customers' information.[34]

The history of the FTC's regulation of online privacy is complex.[35] The FTC's "privacy cases flow from the Agency's decades-long experience and precedent in enforcing false advertising cases . . . [and] the FTC regularly borrows norms developed from the self-regulatory systems of industries and incorporates standards from statutory information privacy law to set standards under the FTC Act."[36] Since 1938, Congress has given the FTC two distinct forms of authority—the power to prevent "unfair or deceptive acts or practices in commerce."[37] FTC privacy law has thus been shaped by theories of unfairness and deception.[38]

The FTC's unfairness authority is governed by a three-part test, which requires that an unfair practice "(1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves and (3) [is] not outweighed by the countervailing benefits to consumers or to competition."[39]

The overwhelming majority of the FTC's privacy enforcement actions have settled.[40] In August 2015, the U.S. Court of Appeals for the Third Circuit

---

[32] 15 U.S.C. § 45(a)(1) (2012).

[33] *Id.* § 45(a)(2).

[34] *See* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1237–38, 1243–45 (2017).

[35] *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145–92 (2016) (explaining the FTC's approach to online privacy regulation); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–89 (2014) (characterizing the FTC's privacy settlements as a form of common law).

[36] HOOFNAGLE, *supra* note 35, at 146.

[37] *See* Pub. L. No. 75-477, 38 Stat. 717 (1938) (codified as amended at 15 U.S.C. § 45(a)(2)).

[38] HOOFNAGLE, *supra* note 35, at 119 ("Theories of unfairness and deception now form the basis of FTC privacy law.").

[39] 15 U.S.C. § 45(n).

[40] *See* Solove & Hartzog, *supra* note 35, at 606–07 ("In nearly all of the FTC's Section 5 cases and complaints alleging violations of COPPA, GLBA, and the Safe Harbor Agreement, the final disposition of the matter is a settlement, default judgment, or abandonment of the action by the FTC in the investigatory stage. The result is that there are hardly any judicial decisions in this arena.").

explicitly ratified the FTC's unfair trade practice theory of cybersecurity liability in an action against Wyndham Worldwide Corp. for a series of extremely egregious information security failures.[41]

The FTC's most expansive theory of liability has recently come under assault. In 2013, the FTC instituted an enforcement action against LabMD, Inc., a medical testing company.[42] The FTC alleged that the company insecurely stored patient information on a peer-to-peer network and argued that lax security practices were an unfair business practice.[43] An administrative law judge ruled against the FTC, concluding that it had failed to show LabMD's security practices had caused or were likely to cause substantial injury to consumers.[44] In July 2016, however, the FTC reversed the administrative law judge, concluding that "the very disclosure of sensitive personal medical information . . . itself represented substantial consumer injury."[45] The company petitioned the U.S. Court of Appeals for the Eleventh Circuit, which issued a unanimous opinion in June 2018 that vacated the FTC's cease and desist order.[46]

The Eleventh Circuit's opinion in *LabMD, Inc. v. FTC* is odd in a couple respects. First, the court did not squarely address whether LabMD's failure to secure patient data constituted an unfair trade practice under Section 5(a). Instead, the court "assume[d] *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice."[47] Because the panel did not squarely confront the question of whether the FTC's enforcement was within its statutory authority, the opinion neither cites nor discusses the Third Circuit's *Wyndham* decision.[48] Second, the court vacated the FTC's cease and desist order, determining that the FTC's remedy—a command that LabMD "overhaul and replace

---

[41] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–47, 249, 259 (3d Cir. 2015) (holding that Wyndham's failure to secure consumer information, which resulted in actual harm to consumers, fell within the plain meaning of "unfair"); *see also* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1194 (2019) ("In the *Wyndham* case, for example, the FTC presented many allegations of atrocious data security practices by the defendant, including the use of out-of-the-box default passwords for servers Wyndham connected to a network, the storage of payment card data in plain text format, and a lack of firewalls and other elementary access controls.").

[42] *See* Complaint, *In re* LabMD, Inc., No. 9357, 2013 WL 523775, at *1 (F.T.C. Aug. 29, 2013).

[43] *See id.* ¶¶ 17–21.

[44] *See In re* LabMD, Inc., No. 9357, 2015 WL 7575033, at *9 (F.T.C. Nov. 13, 2015) ("Complaint Counsel has failed to prove the first prong of [section 45(n)'s] three-part test—that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.").

[45] *In re* LabMD, Inc., No. 9357, 2016 WL 4128215, at *6 (F.T.C. July 28, 2016).

[46] LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018).

[47] *Id.* at 1231.

[48] *See generally id.*

its data-security program to meet an indeterminable standard of reasonableness"—was unenforceable because it was insufficiently specific.[49]

It is uncertain how the FTC will proceed after the Eleventh Circuit's opinion in *LabMD*. There is not a genuine circuit split between the Third Circuit and the Eleventh Circuit, so it seems unlikely that the Supreme Court will weigh in anytime soon.

3. SEC Enforcement

In 2011, the SEC published a guidance document about how federal securities laws apply to data breaches and related instances of information misuse.[50] The document notes that "federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision."[51] Although it concedes that existing disclosure requirements do not expressly refer to cybersecurity incidents, the SEC still requires disclosure of "material information regarding cybersecurity risks and cyber incidents" to prevent misleading the public.[52]

The SEC updated and expanded the guidance in February 2018.[53] The updated guidance says that companies must have "disclosure controls and procedures" in place "that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations."[54] Further, companies are expected "to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences."[55] The SEC also notes that "an ongoing internal or external investigation—which can often be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."[56] And perhaps with an

---

[49] *See id.* at 1236.

[50] Div. of Corp. Fin., *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, U.S. SEC. & EXCHANGE COMM'N (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/HZ66-CG9V] [hereinafter *SEC 2011 Cybersecurity Disclosure Guidance*].

[51] *Id.*

[52] *Id.*

[53] Commission Statement & Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, Release Nos. 33-10459 & 34-82746 (Feb. 26, 2018) [hereinafter *SEC 2018 Cybersecurity Disclosure Guidance*], https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf [https://perma.cc/X99K-HLXV].

[54] *Id.* at 8167.

[55] *Id.* at 8169.

[56] *Id.*

eye to perceptions of impropriety surrounding the Equifax data breach,[57] the agency cautioned that "companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure."[58]

In our analysis of the Yahoo data breaches, my coauthor and I correctly predicted that an SEC enforcement action was inevitable.[59] In April 2018, the SEC "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches."[60]

Some have criticized the SEC because the disclosure standard is so elastic, and action against Yahoo is unlikely to quell that criticism because Yahoo's conduct was so egregious.[61] The settlement is also so miniscule that it borders on meaningless: the Yahoo breach exposed three billion user accounts,[62] meaning that Yahoo paid about one penny for each exposed account.[63]

B. State Law

In the absence of comprehensive information security regulation at the federal level, states have taken the lead experimenting with broadly applicable cybersecurity laws. I discuss three types of state authority below: data security statutes, breach notification statutes, and recent statutory developments.

---

[57] *See* Liz Moyer, *Equifax Special Committee Says Executive Stock Sales Were in the Clear*, CNBC (Nov. 3, 2017), https://www.cnbc.com/2017/11/03/equifax-special-committee-says-executive-stock-sales-were-in-the-clear.html [https://perma.cc/B9KT-RZSV].

[58] *SEC 2018 Cybersecurity Disclosure Guidance*, *supra* note 53, at 8172.

[59] *See* Trautman & Ormerod, *supra* note 34, at 1284–85 ("[T]he SEC appears to have an exceedingly strong case in a future enforcement action against Yahoo. . . . There is very little, if any, language in the SEC's 2011 Guidance that could excuse what currently appears to be a grave misrepresentation [in September 2016] to financial markets, Yahoo's own investors, and the SEC.").

[60] Press Release, U.S. Sec. & Exchange Comm'n, Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71 [https://perma.cc/J3GC-PXAE]; *see also* Altaba Inc., f/d/b/a Yahoo!, Inc., Securities Act Release No. 10485 (Apr. 24, 2018), https://www.sec.gov/litigation/admin/2018/33-10485.pdf [https://perma.cc/3QQA-TNVJ].

[61] *See* Trautman & Ormerod, *supra* note 34, at 1272 (quoting from a September 9, 2017 SEC filing that contains material misrepresentations); *see, e.g.*, Peter J. Henning, *S.E.C.'s New Cybersecurity Guidance Won't Spur More Disclosures*, N.Y. TIMES (Mar. 5, 2018), https://www.nytimes.com/2018/03/05/business/dealbook/sec-guidance-cybersecurity.html [https://perma.cc/6L34-PNZ3].

[62] *See* Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

[63] More precisely: $35,000,000 divided by 3,000,000,000 equals $0.01167.

Thirteen states currently have statutes that require private sector actors to take measures to protect information they collect. The states with data security statutes are: Arkansas,[64] California,[65] Florida,[66] Indiana,[67] Kansas,[68] Maryland,[69] Massachusetts,[70] Nevada,[71] New Mexico,[72] Oregon,[73] Rhode Island,[74] Texas,[75] and Utah.[76]

These statutes are broadly similar, though not monolithic.[77] They usually apply to businesses that collect, maintain, store, or process personal information.[78] The laws also typically require that covered entities implement and maintain reasonable security practices to protect personal information from unauthorized access, use, modification, or disclosure.[79]

All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted breach notification statutes. These laws generally require private and public actors to notify individuals about security breaches that involve the individuals' personally identifiable information.[80]

---

[64] ARK. CODE ANN. § 4-110-104 (2011).

[65] CAL. CIV. CODE § 1798.81.5 (West 2009 & Supp. 2019).

[66] FLA. STAT. § 501.171(2) (West 2017).

[67] IND. CODE § 24-4.9-3-3.5 (West 2018).

[68] KAN. STAT. ANN. § 50-6, 139(b) (Supp. 2018).

[69] MD. CODE COM. LAW §§ 14-3501 to -3503 (LexisNexis 2013).

[70] MASS. GEN. LAWS ch. 93H, § 2(a) (Supp. 2019); *see also infra* Part II.A.2.

[71] NEV. REV. STAT. §§ 603A.210, 603A.215(2) (2005).

[72] N.M. STAT. ANN. § 57-12C-4 (Supp. 2018).

[73] OR. REV. STAT. § 646A.622 (2017).

[74] 11 R.I. GEN. LAWS § 11-49.3-2 (Supp. 2018).

[75] TEX. BUS. & COM. CODE ANN. § 521.052 (West 2015).

[76] UTAH CODE ANN. §§ 13-44-101, -201, -301 (LexisNexis 2013).

[77] For a comparison of these data security statutes, see *Data Security Laws | Private Sector*, NCSL (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/VC2R-GEPF].

[78] *See, e.g.*, KAN. STAT. ANN. § 50-6, 139(b)(1) (2016) (defining a "holder of personal information" to mean "a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person").

[79] *See, e.g.*, N.M. STAT. ANN. § 57-12C-4 (requiring an owner of personal information to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure").

[80] For a list of all fifty-four breach notification laws (including statutory citations), see *Security Breach Notification Laws*, NCSL (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/MA2V-FL8M].

Most of these laws follow a similar pattern: they articulate what kind of entities are required to issue breach notifications,[81] they define what constitutes personally identifiable information[82] and what constitutes a breach,[83] and they provide notification requirements and exemptions.[84]

There have been two recent developments in statehouses worth mentioning—in Vermont and in California.

In May 2018, Vermont enacted a first-in-the-nation regulation overseeing data brokers.[85] The law defines "brokered personal information" to include one or more of the following digitized records about a consumer, if organized for dissemination to third parties: names, addresses, dates of birth, places of birth, mothers' maiden names, unique biometric data, names and addresses of immediate family members, and other information that "would allow a reasonable person to identify the consumer with reasonable certainty."[86] And it defines "data broker" to mean "a business . . . that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."[87] The law also provides examples of what constitutes a direct relationship and some specific exclusions.[88]

The legislation has five primary provisions: (1) it eliminates fees for credit freezes, (2) it requires data brokers to register, (3) it imposes security standards on data brokers, (4) it requires data brokers to report breaches, and (5) it requires data brokers to state their policies on opting out. Much of the law took effect on January 1, 2019.[89]

Meanwhile, in California, an Oakland-based real estate developer named Alastair Mactaggart initiated an effort in 2017 to enact a new state-

---

[81] *See, e.g.*, N.C. GEN. STAT. § 75-65(a) (2009) (requiring "[a]ny business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice" of a security breach); *id.* § 75-61 (providing definitions).

[82] *See, e.g.*, *id.* § 75-61(10) (defining "personal information").

[83] *See, e.g.*, *id.* § 75-61(14) (defining "security breach").

[84] *See, e.g.*, *id.* § 75-65(d)–(e) (prescribing requirements of notice).

[85] *See* H. 764, 2017–2018 Gen. Assemb. (Vt. 2018), https://legislature.vermont.gov/bill/status/2018/H.764 [https://perma.cc/QYX3-CEWX] (reporting that the bill was enacted without the governor's signature on May 22, 2018).

[86] VT. STAT. ANN. tit. 9, § 2430 (1)(A).

[87] *Id.* § 2430(4)(A).

[88] *Id.* § 2430(4)(B)-(C).

[89] *See* H. 764 § 7(b); *see also* VT. OFFICE OF THE ATT'Y GEN., GUIDANCE ON VERMONT'S ACT 171 OF 2018 DATA BROKER REG. (2018), https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf [https://perma.cc/VH56-HBXB].

law digital privacy statute using California's ballot initiative mechanism.[90] The ballot initiative had three primary components: First, it proposed to give consumers the right to request that companies disclose what data the company has collected on the consumer.[91] Second, it proposed to give consumers the right to demand that companies not sell their data or share it with third parties for business purposes.[92] Third, it proposed to give consumers the right to sue or fine companies that violate the law.[93] By March 2018, the ballot initiative had amassed over 600,000 signatures, well above the 366,000 minimum required for the measure to appear on the November 2018 ballot.[94]

In June 2018, however, in exchange for Mr. Mactaggart's agreement to revoke the ballot initiative, California's state legislature enacted a digital privacy statute that was modeled on the ballot initiative.[95] The new law gives consumers the right to know what information a company is collecting about them, why the company is collecting the information, and with whom the company plans to share that information.[96] Consumers may also demand that a company delete their information or demand that a company not sell or share their information.[97] Further, the law forbids companies from discriminating against consumers who exercise their rights under the law.[98] The statute is scheduled to go into effect in January 2020.[99]

There is one glaring difference between the proposed ballot initiative and the legislature-enacted law: the latter does not provide consumers the right to file suit against companies that do not comply with the law.[100] Instead,

---

[90] Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html [https://perma.cc/P33J-MHNC].

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] Press Release, Californians for Consumer Privacy, California Consumer Privacy Act Clears Major Hurdle: Submits 629,000 Signatures Statewide (May 3, 2018), https://www.caprivacy.org/post/california-consumer-privacy-act-clears-major-hurdle-submits-625-000-signatures-statewide [https://perma.cc/3AEV-B8UG].

[95] Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://nyti.ms/2lEdwdX [https://perma.cc/2S98-LNUN].

[96] A. B. 375 § 2(i), 2017–2018 State Assemb. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 [https://perma.cc/9X7Z-4FAS].

[97] *See id.* § 1798.105.

[98] *See id.* § 1798.125.

[99] *See id.* § 1798.198.

[100] There is, however, an ongoing fight to add a private enforcement provision to the law. *See* Jill Cowan, *The Fight Over a Landmark Digital Privacy Law*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/us/digital-privacy-hannah-beth-jackson-ccpa.html [https://perma.cc/ELT4-TLC3] (interviewing the bill's sponsor, Cal. State Senator Hannah-Beth Jackson).

the new law gives the California Attorney General some new authority to fine companies that fail to comply.[101]

The California Consumer Privacy Act, as the new law is known, represents the most significant domestic substantive digital privacy law successfully enacted to date. But as I argue at length throughout this Article, stripping out the right of private enforcement is both telling and significant.[102]

C. Foreign Law

On April 14, 2016, the European Parliament approved the General Data Protection Regulation (GDPR).[103] The GDPR replaced Directive 95/46/EC—known as the Data Privacy Directive—and the GDPR went into effect on May 25, 2018.[104]

The European Union's GDPR is relevant to this survey of the domestic regulatory environment for two primary reasons. First, it is the broadest and most aggressive form of data privacy regulation to date.[105] Second, it has significant extraterritorial reach because GDPR standards apply to the personal information of EU Internet users no matter the location of the entity that possesses the information.[106]

The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person."[107] The GDPR guarantees several privacy rights to EU Internet users; these include the right to be notified about a security breach,[108] the right to access information,[109] the right to erasure

---

[101] *See, e.g.*, A. B. 375 § 1798.150.

[102] One need not be particularly cynical to understand why the technology lobby trained its most strenuous objection on the ballot initiative's private right of enforcement. *See, e.g.*, *infra* Part II.A.

[103] Regulation (EU) 2016/679, of the European Parliament and 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, 2016 O.J. (L 119) [hereinafter GDPR], https://gdpr-info.eu/ [https://perma.cc/2G8Z-5PVM].

[104] *See id.*, Recital No. 171.

[105] *See* Chris Mirasola, *Summary: The EU General Data Protection Regulation*, LAWFARE (Mar. 1, 2018), https://www.lawfareblog.com/summary-eu-general-data-protection-regulation [https://perma.cc/JSF3-5W5X]; Adam Satariano, *What the G.D.P.R., Europe's Tough New Data Law, Means for You*, N.Y. TIMES (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html [https://perma.cc/Y23L-C59K].

[106] GDPR, *supra* note 103, Recital No. 23; *GDPR FAQs*, https://www.eugdpr.org/gdpr-faqs.html [https://perma.cc/795E-4S4J] ("[GDPR] applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.").

[107] *See* GDPR, *supra* note 103, Art. 4(1).

[108] *See id.*, Art. 33.

[109] *See id.*, Art. 15.

(a.k.a. the right to be forgotten),[110] and the right to data portability,[111] among others.[112]

The GDPR has strong consent requirements. "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of [a person's] agreement to the processing of personal data relating to him or her."[113] For some categories of information (e.g., race, political opinion, religious belief, genetic information, biometric data) explicit, affirmative consent (opt-in) is required.[114]

Violations of the GDPR may result in harsh penalties: Authorities may impose administrative fines of up to four percent of a company's global annual revenue for some violations of the GDPR's provisions.[115]

There is significant uncertainty about the GDPR's applicability and scope.[116] Many companies have been under pressure to make the features required by the GDPR a global baseline.[117] But so far, companies have not adopted global GDPR compliance. In January 2019, France announced the first major GDPR penalty against Google for $57 million.[118]

---

[110] *See id.*, Art. 17.

[111] *See id.*, Art. 20.

[112] *See, e.g.*, *id.*, Art. 16 (right to rectification); *id.*, Art. 18 (right to restriction of processing); *id.*, Art. 21 (right to object).

[113] *Id.*, Recital No. 32.

[114] *See id.*, Art. 9.

[115] *See id.*, Art. 83(5)–(6). This could result in significant penalties for the wealthiest companies. For example, Facebook could be fined $1.63 billion for a 2018 security breach. *See* Sam Schechner, *Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach*, WALL ST. J. (Sept. 30, 2018), https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906; *see also infra* note 118 and accompanying text (noting that Google faced a GDPR fine of up to $4.7 billion).

[116] *See, e.g.*, Nick Ismail, *GDPR Uncertainty and Confusion Remains*, INFO. AGE (Sept. 13, 2017), http://www.information-age.com/gdpr-uncertainty-remains-123468541/ [https://perma.cc/2HVM-CTZK] (discussing findings from a survey that says thirty-seven percent of respondents do not know whether their companies need to comply with GDPR and twenty-eight percent believe they do not need to comply).

[117] *See, e.g.*, Natasha Lomas, *Facebook Urged to Make GDPR Its "Baseline Standard" Globally*, TECHCRUNCH (Apr. 9, 2018), https://techcrunch.com/2018/04/09/facebook-urged-to-make-gdpr-its-baseline-standard-globally/ [https://perma.cc/ZS8P-NQ7X]. This phenomenon is sometimes referred to as the "Brussels Effect," which "operates principally as a *de facto* mechanism, when market actors conform their global products to European rule." *See* Anupam Chander et al., *Catalyzing Privacy Law*, GEO. L. FAC. PUBLICATIONS & OTHER WORKS, 10–11 (2019), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3208&context=facpub [https://perma.cc/78W9-D4BK].

[118] Tony Romm, *France Fines Google Nearly $57 Million for First Major Violation of New European Privacy Regime*, WASH. POST (Jan. 21, 2019), https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

II. Information Misuse as a Market Failure

Despite this patchwork of authorities derived from federal, state, and foreign law, data breaches and information misuse remain a constant and pervasive phenomenon of modern life.[119] Section A of this Part models investment in information security as a function of profit and cost.[120] Section B uses that model to identify what is animating these pervasive information security failings.[121]

A. Security, Profit, and Cost

In my investigation and analysis of the Yahoo data breaches, a pair of anecdotes looms large. First, in 2014, Yahoo's then-new Chief Information Security Officer Alex Stamos pressed senior management to adopt end-to-end encryption for the company's entire digital infrastructure.[122] Yahoo's then-Senior Vice President Jeff Bonforte balked; because end-to-end encryption would block the company from indexing and searching the contents of users' message data, Bonforte argued that the company should not lose the ability to use that data to tailor advertisements.[123]

Second, following disclosure to senior management of a system-wide exfiltration of users' email accounts, Yahoo's then-CEO Marissa Mayer refused to implement one of the most basic security measures that security experts consider standard practice following a breach: automatically resetting all users' passwords.[124] Mayer's rationale for rejecting this fundamental staple of data breach response was derived from a "fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services."[125]

---

[119] *See supra* notes 20–118 and accompanying text.

[120] Other scholars have helpfully used economic concepts and models to elucidate the market forces around privacy. *See generally* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015) (explaining that the loss of privacy and obscurity is a function of the decreased transaction costs of surveillance and information collection); *Obscurity Settings: Episode 58*, ORAL ARGUMENT (Apr. 24, 2015), https://oralargument.org/58 [https://perma.cc/C57E-RYR6]; *see infra* notes 122–128 and accompanying text.

[121] *See infra* notes 129–138 and accompanying text.

[122] Nicole Perlroth & Vindu Goel, *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say*, N.Y. TIMES (Sept. 28, 2016), http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html [https://perma.cc/H3LR-MUXA].

[123] *Id.* For his part, Mr. Bonforte later confirmed this report. Answering a question about his resistance to Mr. Stamos's end-to-end encryption effort, Mr. Bonforte replied, "I'm not particularly thrilled with building an apartment building which has the biggest bars on every window." *Id.*; *see also* Victoria L. Schwartz, *Corporate Privacy Failures Start at the Top*, 57 B.C. L. REV. 1693, 1697 (2016) (arguing that another reason why corporations fail to adequately safeguard personal information is due to corporate executives' "reduced privacy preference[s]," which may lead them to "undervalue or not even recognize the privacy implications of their business decisions").

[124] Perlroth & Goel, *supra* note 122.

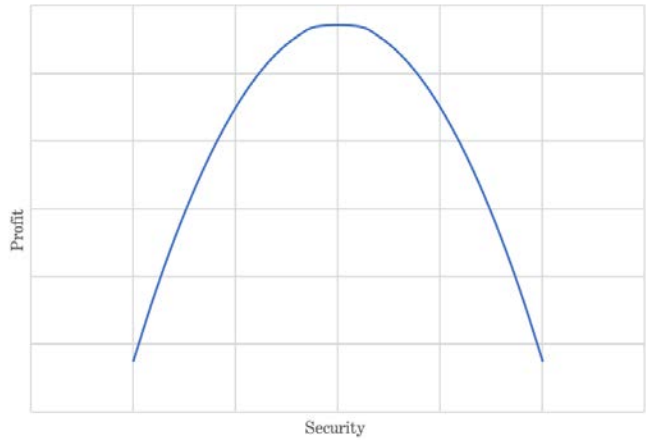
[125] *Id.*

These two anecdotes starkly demonstrate the trade-off between profit and security. Too-little security can cost an organization. Examples here include data breaches and damaging disclosures of information misuse. These have direct costs (e.g., defending against litigation and enforcement actions) and opportunity costs (e.g., dissuading potential users and customers from using the company's services because of its abysmal security practices).

But less well-explored is that too-much security can also prove costly. How? Mayer's and Bonforte's resistance to standard security practices is illustrative: Investing too heavily in security also has both direct costs (outlays for security services, software, vendors, and employees) and opportunity costs—such as diminished usability (restricting account recovery options and abilities,[126] instituting multi-factor authentication, requiring complex passwords) and lost revenue streams (end-to-end encryption thwarting tailored marketing).

In my analysis of the Yahoo data breaches, I developed a simple model to capture this trade-off.[127] It expresses investment in information security as a function of a company's profit:

Figure 1: The Profit-Maximizing Model of Security



But the model is not limited to for-profit companies.[128] Security investment can also be expressed as a function of cost:

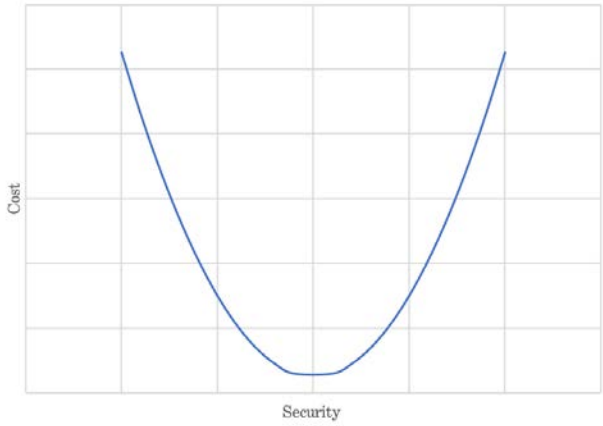
---

[126] Feigning forgotten login credentials is one of the most tried and true ways that hackers exploit vulnerabilities and gain access to user accounts. Companies have responded by making it more difficult to reset login credentials, but this has the side effect of keeping out legitimate users too. *See, e.g.*, *Advanced Protection Program*, GOOGLE, https://landing.google.com/advancedprotection/ [https://perma.cc/FMM9-G8AP] ("If you have lost both keys and do not have access to a logged-in session, you will need to submit a request to recover your account. It will take a few days for Google to verify it's you and grant you access to your account.").

[127] *See* Trautman & Ormerod, *supra* note 34, at 1289–91.

[128] *See* Lawrence J. Trautman & Janet Ford, *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 971, 1033–35 (2019).

Figure 2: The Cost-Minimizing Model of Security



The top and bottom of the parabolas, respectively, are the equilibria. In the former, the top of the parabola is the profit-maximization amount of security; in the latter, the bottom of the parabola is the cost-minimization amount of security. In both, any more or any less security would lower the company's profit and increase its costs. A failure to invest in enough security is a left-side disequilibrium, or "too-little security disequilibrium." And investing in too much security is a right-side disequilibrium, or "too-much security disequilibrium."

B. Disequilibrium and Information Misuse

Too-little security disequilibrium and too-much security disequilibrium present distinct challenges to organizations. But society collectively spends much more time concerned with the former versus the latter. Why?

As an initial matter, it is important to note that it is unlikely that too-much security disequilibrium is more costly and dire—if anything, the opposite may be true. Nearly every metric of losses to identity theft increases year-over-year, sometimes by double-digit percentages.[129] In 2017, there were an average of 245 curated breaches each month, or eight curated breaches each

[129] *See* Robert N. Charette, *2017 Was a Record Year for ID Theft in the U.S.*, IEEE SPECTRUM (Feb. 23, 2018), https://spectrum.ieee.org/riskfactor/computing/it/2017-is-another-us-record-year-in-id-information-thefts [https://perma.cc/V3AU-V3YH] (summarizing annual estimates from Javelin Strategy & Research); Press Release, Javelin Strategy, Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new [https://perma.cc/CW2P-ZLWG].

day.[130] Of 8.7 billion raw records exposed in 2017, over three billion were real and unique identities—a sixty-four percent increase from 2016.[131] Approximately 15.4 million Americans were victims of identity theft in 2016, a sixteen percent increase over 2015.[132] In 2017, that number was at least 16.7 million.[133] In 2015, identity thieves stole $15.5 billion, which increased to $16.2 billion in 2016 and $16.8 billion in 2017.[134] And identity theft alone does not capture the full range of costs and harms that information misuse inflicts on consumers and users.[135]

Rather, there are three primary differences—or asymmetries—between too-little security and too-much security disequilibria: who bears the cost, the variability of the marginal cost, and information imperfection. Together, these asymmetries foster a lopsided incentive structure that favors too-little security.

First, information misuse (i.e., too-little security disequilibrium) does cost companies, but the company does not exclusively bear those costs. Instead, the costs of too-little security disequilibrium are shared between the company and the consumers whose information is misused or compromised—a classic negative externality.[136]

"[T]he incentive for most firms is to invest in very basic security—only enough to secure their systems from casual attackers—and otherwise pay no attention to security."[137] Even upon widespread adoption of breach notification laws, "firms still do not face substantial incentives to adopt strong security practices," which "is in part because there is still little likelihood that a firm will be held liable for damages resulting from a data breach."[138]

---

[130] *See 2018 4iQ Identity Breach Report*, *supra* note 7, at 10. The report explains that curated data breach is one in which real and unique identities are likely to have been exposed. *See id.* at 9–10.

[131] *Id.* at 5.

[132] Charette, *supra* note 129.

[133] *Id.*

[134] *Id.*

[135] Other costs include, for example, the time, effort, and money that consumers spend on prophylactic measures like credit monitoring. One company estimated that the market for services that purport to protect against identity theft in 2015 was $3.8 billion, an eighteen percent increase from 2014. *See* E.J. Schultz, *Be Afraid, Be Very Afraid: ID Theft Protectors Want to Scare the Money from Your Wallet*, ADAGE (Jan. 9, 2018), http://adage.com/article/cmo-strategy/afraid-id-theft-protectors/311840/ [https://perma.cc/GUX3-EVVY].

[136] Jim Daly, *Expenses from the Home Depot and Target Data Breaches Surpass $500 Million*, DIGITAL TRANSACTIONS (May 26, 2016), https://www.digitaltransactions.net/expenses-from-the-home-depot-and-target-data-breaches-surpass-500-million/ [https://perma.cc/U2QJ-T976] (estimating that a 2013 breach of 40 million customers' payment card information and an additional 70 million customers' personal information cost Target $291 million); *see* Johannes M. Bauer & Michael J.G. van Eeten, *Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options*, 33 TELECOMM. POL'Y 706, 707 (2009).

[137] Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1511 (2017).

[138] *Id.*

In contrast, the costs of too-much security disequilibrium are shouldered by the company alone: Shareholders, not consumers, suffer from duplicative spending on security services and lost opportunities to monetize information within the company's reach. More to the point, these metrics are easy to measure and simple to tweak to satisfy shareholders' interests—which is to say that they are self-correcting. Too-much security disequilibrium is less likely to persist because a company's management (in discharging their fiduciary duties to shareholders) has strong incentives to correct them and they are comparatively easy to correct.

Second, to be sure, both types of disequilibria are difficult to assess ex ante. But the stakes for too-little security disequilibrium are considerably higher. In other words, the marginal cost of too-much security disequilibrium is relatively low and consistent. On the other hand, the marginal cost of too-little security disequilibrium is extremely variable: spending one fewer dollar on security may cost the company nothing, or it may be the dollar that would have averted a massive data breach.

The result is a second asymmetry. Over time, shareholders and their fiduciaries are likely to exert persistent, incremental downward pressure on information security spending—particularly if the company has not suffered from an information misuse incident during the relevant period. The Yahoo anecdotes starkly illustrate this dynamic. Only after a costly misuse incident will there be any pressure to invest in greater security.

Third, imperfect information also likely plays a role in the prevalence of too-little security disequilibrium. This is a third asymmetry: shareholders and management can more easily measure the cost of too-much security disequilibrium than too-little security disequilibrium. Losses from an information misuse incident are impossible to predict. Some of the potential variables include how many people the misuse affects; the magnitude of the misuse; competition in the relevant market; the bad publicity; the reputational harm; the expenditures on lawyers, litigation, investigation, and penalties; the likelihood of class action litigation's success; and more.

In sum, there are significant differences between what happens when a company spends too little on security versus when a company spends too much on security. The takeaway is that too-little security disequilibrium—i.e., data breaches and other episodes of information misuse—are far more likely to occur, and they are more likely to reoccur.

III. A Private Enforcement Remedy

Public policy should change and seek to correct information misuse disequilibrium. In this Part, I propose a specific form for that change: one or more states should enact legislation that imposes a fiduciary duty on anyone who

collects or retains personally identifiable information. The legislation should create a cause of action for breach of that duty, impose strict liability on violators of the duty, and prescribe damages that increase with a defendant's culpability. I refer to this remedial scheme as a private enforcement remedy.

Section A of this Part describes the proposed right and the proposed remedy.[139] Section B provides the rationale for each component of the proposed remedial scheme.[140]

A. The Right

One or more states should enact legislation that imposes a fiduciary duty on any entity that collects, retains, processes, sells, or shares personal information. I refer to covered entities as information fiduciaries and refer to a person whose information is collected as the principal.

The statute should impose several duties on information fiduciaries, some general and others specific. General duties include analogs to other fiduciary relationships, like a duty of care, a duty of loyalty, a duty to use the information for the principal's benefit and not to the principal's disadvantage.[141]

These general duties should give rise to concrete rules in specific situations. For starters, the principal should have primary discretion about whether he or she wants an information fiduciary to collect and retain a given piece of information, which means explicit opt-in rather than opt-out. This also means that an information fiduciary should only use a principal's personally identifiable information in a way that the principal has explicitly opted in to. So, if an information fiduciary wants to use a principal's information for a new, different, or otherwise unauthorized use, the information fiduciary should be required to obtain new, explicit, opt-in consent. Ideally, the right of the private enforcement remedy would require opt-in consent requirements which would mirror the express consent requirements of the GDPR.[142]

The statute should also expressly set the standard of care for information misuse. Massachusetts, for example, has adopted regulations under its information security statute that prescribe a process-based approach to information security.[143] I have written elsewhere about these Written Information

---

[139] *See infra* notes 141–149 and accompanying text.

[140] *See infra* notes 150–155 and accompanying text.

[141] *See* Balkin, *supra* note 9, at 1204, 1208–09; *see also* RESTATEMENT (SECOND) OF TORTS § 865 (AM. LAW. INST. 1979); *infra* Part IV.B.2.

[142] *See* GDPR, *supra* note 103, Recital No. 32; *see id.*, Art. 9; *see also supra* Part I.C.

[143] *See* 201 MASS. CODE REGS. § 17.00 (2009).

Security Protocols (WISPs),[144] and the Massachusetts regulation is an illustrative example of how a jurisdiction could use the WISP framework to set the relevant standard of care for information misuse. Under the regulation, covered entities must "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."[145] The regulation also includes some specific procedural requirements, like designating a security officer, regularly monitoring and updating the program, and documenting any responsive actions.[146] A Massachusetts regulatory agency created a data security compliance checklist and a frequently asked questions document to help businesses comply with these requirements.[147] As several scholars have noted, over time, a nebulous "reasonableness" requirement has increasingly given way to concrete rules for data security compliance.[148]

Breach notification laws should also be expanded to require notice for all types of information misuse. As detailed below, robust breach notification is critical, because receipt of notification would be sufficient to establish strict liability. Incentives under the current state of affairs and under this proposal strongly discourage a company discovering a breach.[149]

The GDPR punishes failure to notify harshly, which has the advantage of reshaping incentives in favor of prompt breach discovery and notification. This remedial scheme should also provide users with the ability to seek punitive damages for a company's noncompliance with broad information misuse notification requirements.

Plaintiffs should thus be empowered to sue to enforce two complementary rights—breach of an information fiduciary duty and failure to notify—and the culpability schedule detailed below should apply to both of these rights.

B. The Remedy

The structure of the remedy is perhaps more important than the specific contours of an information fiduciary's duties. Why? For one, many laws—both federal and state—impose some requirements on those who collect and retain information. The problem is a dearth of remedies.[150]

---

[144] *See* Trautman & Ormerod, *supra* note 34, at 1241–43.

[145] 201 MASS. CODE REGS. § 17.03(1).

[146] *Id.* § 17.03(2).

[147] *See 201 CMR 17.00 Compliance Checklist*, MASS. OFF. OF CONSUMER AFF. & BUS. REG., https://www.mass.gov/files/documents/2017/11/21/compliance-checklist.pdf [https://perma.cc/XWB9-RWXV]; *Frequently Asked Questions Regarding 201 CMR 17.00*, MASS. OFF. OF CONSUMER AFF. & BUS. REG., https://www.mass.gov/files/documents/2018/03/21/201%20CMR%2017%20FAQs%202018_0.pdf [https://perma.cc/GC4G-ZX62].

[148] *See, e.g.*, McGeveran, *supra* note 41, at 1193–95 (listing "worst practices").

[149] *See supra* note 137 and accompanying text.

[150] *See* Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN. ST. L. REV. 1, 4–5 (2008).

The breach of an information fiduciary's duty should be enforceable by anyone whose information is misused. As an information fiduciary becomes more culpable for a breach, the penalties should ratchet up. Here is a proposed schedule:

Figure 3: Proposed Penalty Schedule

Culpability	Primary Penalty	Secondary Penalty
Strict Liability	• Nominal damages paid to litigants; or • Declaratory judgment; or • A judicially determined penalty constituting "meaningful deterrence" that is paid to the state treasury	Reasonable attorney's fees and costs
Negligence	• Statutorily prescribed compensatory damages paid to the affected class, or, alternatively, paid to the litigants and to the state treasury; and/or • A judicially determined penalty constituting "meaningful deterrence" that is paid to the state treasury	Reasonable attorney's fees and costs
Recklessness	• Statutorily prescribed compensatory damages paid to the affected class, or, alternatively, paid to the litigants and to the state treasury; and • A judicially determined penalty constituting "meaningful deterrence" that is paid to the state treasury	Reasonable attorney's fees and costs
Knowledge and purpose	• Statutorily prescribed compensatory damages and punitive damages paid to the affected class, or, alternatively, paid to the litigants and to the state treasury; and • A judicially determined penalty constituting "meaningful deterrence" that is paid to the state treasury	Reasonable attorney's fees and costs

Under this schedule, an information fiduciary is strictly liable for information misuse. But strict liability may result in only nominal damages (or a declaratory judgment). In other words, companies that misuse information must pay private attorneys general to sue them; if discovery in that litigation reveals no more culpability than strict liability, then the information fiduciary may be liable for reasonable attorney's fees and little else.[151] If, however, the trial judge determines that nominal damages and reasonable attorney's fees would not constitute a meaningful deterrent against future information mis-

[151] *See* David Shub, *Private Attorneys General, Prevailing Parties, and Public Benefit: Attorney's Fees Awards for Civil Rights Plaintiffs*, 42 DUKE L.J. 706, 708–09 n.10 (1992) (tracing the term "private attorney general" to *Associated Indus. of New York State v. Ickes*, 134 F.2d 694, 704 (2d Cir. 1943)).

use, the judge should be empowered to order a penalty fee that would constitute a meaningful deterrent, which the company would pay to the state treasury.[152]

If discovery uncovers negligence, then the defendant is liable for reasonable attorney's fees and statutorily prescribed compensatory damages. The defendant should pay these damages to the affected class, or—if distribution to the class is impracticable—the defendant should compensate the named plaintiffs and pay the remaining damages to the state treasury.[153] The judicially determined "meaningful deterrent" mechanism should also apply as a fallback option here.

If, instead, discovery uncovers recklessness, the information fiduciary is liable for reasonable attorney's fees, statutorily prescribed compensatory damages paid to the affected class (or to named plaintiffs and the treasury), plus an additional penalty fee owed to the state treasury. Further, if discovery uncovers knowledge or purposefulness, then the defendant is liable for both statutorily prescribed compensatory and punitive damages paid to the affected class (or to named plaintiffs and the treasury), a penalty fee paid to the state treasury, plus reasonable attorney's fees.

The appeal of this proposed schedule has everything to do with influencing information fiduciaries' behavior and deterring information misuse; compensating victims of information misuse is an ancillary benefit.

This remedial scheme differs from other contexts that use strict liability in one important respect. In products liability, the plaintiff obtains compensatory damages upon establishing strict liability, so there is no reason to argue for negligence in the alternative. Under this proposal, a plaintiff should be entitled to argue in the alternative for both negligence and strict liability because the differing levels of culpability result in differing levels of damages.

The Third Restatement of Torts argues that courts should not submit to the fact-finder multiple differently labeled theories of liability using identical facts because allowing "two or more factually identical risk-utility claims to go to a jury under different labels . . . would generate confusion and may well

---

[152] This judicial fallback mechanism ensures that even the largest and wealthiest companies face a penalty that has some incentive-shifting teeth. The GDPR, for example, accomplishes this same objective using a different mechanism: It authorizes penalties up to four percent of a company's global annual revenues. *See supra* note 115 and accompanying text.

[153] Sometimes courts order *cy pres* settlements in class actions when it's impracticable to distribute a reward or settlement to the class. The Supreme Court has recently signaled its interest in this issue. *See* Frank v. Gaos, 869 F.3d 737 (9th Cir. 2017), *vacated and remanded*, 139 S. Ct. 1041 (2019). To avoid the problems posed by *cy pres* settlements and the appearance of conflicts of interest, courts—in cases where it's impracticable to distribute these statutorily prescribed damages to the class—should merely order defendants to pay the damages to the state treasury.

result in inconsistent verdicts."[154] In other words, the plaintiff in a products liability case should not be permitted to argue that the defendant is strictly liable, or, in the alternative, that the defendant was negligent. At the same time, the Restatement acknowledges that "as long as the requisites [of strict liability] are met, the plaintiff may in appropriate instances—for example, in connection with comparative fault or punitive damage claims—show that the defect resulted from reckless, willfully indifferent, or intentionally wrongful conduct of the defendant."[155]

The proposed information misuse remedy would allow the plaintiff to argue in the alternative for any combination of culpability. The Restatement's concerns are legitimate when plaintiffs already obtain compensatory damages under strict liability, but they are inapposite here. With information misuse, defendants will have a statutory obligation to notify users about instances of information misuse. The fact that a company has notified users is, by itself, enough to establish strict liability. But that strict liability may only result in nominal damages; plaintiffs will need to establish greater culpability to recover compensatory damages. Following discovery and litigation under this scheme, the plaintiff should be free to argue that the defendant was, for example, negligent or reckless, and different findings of culpability are accompanied by statutorily prescribed damages.

In sum, plaintiffs in products liability obtain compensatory damages upon establishing strict liability, so arguing for negligence promotes confusion without any accompanying change in damages. Here, strict liability only imposes nominal damages, so plaintiffs should be permitted to argue for negligence and its accompanying compensatory damages.

* * *

The proposed remedial scheme has four essential components: it should be created under state law; it should impose a fiduciary duty on entities that collect or retain personally identifiable information; it should hold defendants strictly liable for information misuse; and it should prescribe a schedule of damages that begins with nominal damages and attorney's fees for strict liability and ratchets up damages with a defendant's culpability.

IV. JUSTIFICATIONS

This Part provides the rationale for each of the four essential components of the private enforcement remedy described in the previous section.

---

[154] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 cmt. n. (AM. LAW. INST. 2019).

[155] *Id.*

Section A of this Part discusses why the private enforcement remedy must be enacted and implemented under state law.[156] Section B argues that the private enforcement remedy should impose a fiduciary duty on entities that collect and use information about users.[157] Section C asserts that this fiduciary duty must be combined with the imposition of strict liability to give the tort some teeth.[158] Section D discusses why the private enforcement remedy should only impose nominal damages.[159]

A. Why State Law?

The private enforcement remedy should be enacted and implemented under state law. Federal courts, led by the U.S. Supreme Court, have narrowly interpreted the "injury-in-fact" requirement of Article III's "case or controversy" requirement. This slender interpretation of justiciable disputes sharply limits Congress's ability to create private enforcement vehicles.[160] And perhaps more to the point, uncertainty about whether a litigant has standing in a data misuse case would wholly undermine the deterrence and incentive-altering purposes of the remedy.

1. Statutory Standing Before *Spokeo*

The Supreme Court's standing jurisprudence has two distinct strains that conflict with one another.[161] On the one hand is Proposition A: "that the content of an injury is shaped by law, and therefore by Congress."[162] On the other is Proposition B: that some of Congress's attempts to shape and create injuries by statute violate Article III's case-or-controversy requirement.[163]

The Court's 1998 decision in *FEC v. Akins* provides an instructive example of Proposition A.[164] In that case, a group of voters brought suit against the Federal Election Commission (FEC) to challenge the FEC's determination that the American Israel Public Affairs Committee (AIPAC) was not a "political committee" within the meaning of a statute and thus not subject to

---

[156] *See infra* notes 160–241 and accompanying text.

[157] *See infra* notes 243–291 and accompanying text.

[158] *See infra* notes 293–307 and accompanying text.

[159] *See infra* notes 309–318 and accompanying text.

[160] *See generally* Amy Grewal Dunn, *Bridging the Gap: How the Injury Requirement in FTC Enforcement Actions and Article III Standing Are Merging in the Data Breach Realm*, 20 J. CONSUMER & COM. L. 9 (2016).

[161] William Baude, *Standing in the Shadow of Congress*, 2016 SUP. CT. REV. 197, 199 (2017).

[162] *Id.*

[163] *Id.*

[164] FEC v. Akins, 524 U.S. 11 (1998).

disclosure requirements.[165] The Court held that the challengers had standing because "[t]he 'injury in fact' that [the challengers] have suffered consists of their inability to obtain information . . . that on [their] view of the law, the statute requires that AIPAC make public."[166]

The Court rejected the FEC's argument that the challengers had only a "generalized grievance," because that concern "invariably appears in cases where the harm at issue is not only widely shared, but is also of an abstract and indefinite nature."[167] It acknowledged that a widely shared injury is often correlated with an abstract injury but concluded that "their association is not invariable, and where a harm is concrete, though widely shared, the Court has found 'injury in fact.'"[168] To support that conclusion, the majority analogized the challenger's position to an example where "large numbers of individuals suffer the same common-law injury (say, a widespread mass tort)."[169]

The most prominent example of Proposition B is *Lujan v. Defenders of Wildlife*, which the Court decided in 1992, a few years before *Akins*.[170] *Lujan* denied standing to an environmental group that sought to challenge a regulation under the Endangered Species Act.[171] The Court flatly rejected the suggestion that Congress could use a citizen-suit provision to create a right to have the Executive Branch observe the procedures required by the statute. The Court noted: "[T]here is absolutely no basis for making the Article III inquiry turn on the source of the asserted right," because it would violate separation-of-power principles "[t]o permit Congress to convert the undifferentiated public interest in executive officers' compliance with the law into an 'individual right' vindicable in the courts."[172]

In 2009, the Court came to the same conclusion in *Summers v. Earth Island Institute*.[173] *Summers* closely resembles *Lujan*: An environmental group sued to challenge a procedural defect in an environmental regulation. But the Court's conclusion seemed to sweep far more broadly than procedural compliance in environmental law; as the Court stated, "[i]t makes no difference that the procedural right has been accorded by Congress."[174]

---

[165] *Id.* at 13–14.
[166] *Id.* at 21.
[167] *Id.* at 23–24.
[168] *Id.* at 24.
[169] *Id.*
[170] Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).
[171] *Id.* at 558.
[172] *Id.* at 576.
[173] Summers v. Earth Island Inst., 555 U.S. 488 (2009).
[174] *Id.*

2. *Spokeo v. Robins*: An Unresolved Tension

In 2016, the Court decided *Spokeo v. Robins*.[175] *Spokeo* asked whether the plaintiff had Article III standing under a provision of the Fair Credit Reporting Act (FCRA) that creates a private right of action.[176] Specifically, the FCRA provides that "[a]ny person who willfully fails to comply with any requirement [of the FCRA] with respect to any [individual] is liable to that [individual]."[177] The statute prescribes damages where the non-complying agency is liable to the individual for either actual damages or statutory damages of $100 to $1,000 per violation, plus attorney's fees, costs, and potentially punitive damages.[178] In *Spokeo*, the defendant, a consumer reporting agency, made numerous inaccurate representations about the plaintiff, including "that he is married, has children, is in his 50s, has a job, is relatively affluent, and holds a graduate degree."[179] According to the plaintiff, all of that information was false.[180]

The district court dismissed the complaint, but the U.S. Court of Appeals for the Ninth Circuit reversed, holding that the plaintiff had standing.[181] The panel noted that Article III limits Congress's power to confer standing but that "the violation of a statutory right is usually a sufficient injury in fact to confer standing."[182] The Ninth Circuit held that the plaintiff had suffered sufficient harm because he alleged that the defendant "violated his statutory rights, not just the statutory rights of other people," and because his interests "in the handling of his credit information are individualized rather than collective."[183]

The Supreme Court vacated the Ninth Circuit's decision and remanded the case, determining that the panel's "analysis focused on the second characteristic (particularity), but it overlooked the first (concreteness)."[184]

The tension between Proposition A and Proposition B is palpable in the Court's opinion. On the one hand, the Court noted that "Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."[185] On the other hand, the Court acknowledged that "Congress has the power to define injuries

---

[175] Spokeo v. Robins, 136 S. Ct. 1540 (2016).
[176] *Id.* at 1544.
[177] 15 U.S.C. § 1681n(a) (2012).
[178] *Id.*
[179] *Spokeo*, 136 S. Ct. at 1546.
[180] *Id.*
[181] Robins v. Spokeo, 742 F.3d 409, 414 (9th Cir. 2014).
[182] *Id.* at 412–13.
[183] *Id.* at 413.
[184] *Spokeo*, 136 S. Ct. at 1545.
[185] *Id.* at 1547 (quoting Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997)).

and articulate chains of causation that will give rise to a case or controversy where none existed before."[186] According to the majority, "Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law."[187]

In his majority opinion, Justice Alito held that "[c]oncreteness . . . is quite different from particularization" and that not all statutorily defined rights are sufficiently concrete to satisfy Article III.[188] What makes some statutory rights sufficiently concrete that other statutory rights lack? It is not clear. The Court held that, to be concrete, an injury "must actually exist," and that it must be "real, and not abstract."[189] At the same time, the Court said that a concrete injury may be "intangible" and may be based on a "risk of real harm."[190] As one scholar has observed, "[t]he Court did not explain, however, why some statutory rights are not 'real,' especially when some intangible harms apparently can be."[191]

3. Information Misuse Standing After *Spokeo*

Spokeo has not resolved much. The lower courts continue to divide over how to apply these two distinct lines of cases in the context of information misuse. The Court declined the invitation to resolve data breach standing cases in 2017,[192] 2018,[193] and 2019.[194] Below is a discussion of two categories of post-*Spokeo* data misuse standing cases from the lower federal courts. The first category is a series of cases arising from data breaches and plaintiffs' claims about future harm. The second category includes several cases about information collection and misuse in violation of a statute. In both, courts have generally—though not uniformly—agreed with defendants' arguments that the plaintiffs lack Article III standing. In the third section, I discuss a few cases where lower courts have analogized statutory violations to common-law privacy torts and identify an important development at the Supreme Court.

---

[186] *Id.* at 1555 (Kennedy, J., concurring in part and concurring in judgment) (quoting *Lujan*, 504 U.S. at 580).

[187] *Id.* at 1549 (majority opinion) (quoting *Lujan*, 504 U.S. at 578).

[188] *Id.* at 1550.

[189] *Id.* at 1548 (internal quotation marks omitted).

[190] *Id.*

[191] Baude, *supra* note 161, at 215.

[192] *See* Beck v. McDonald, 848 F.3d 262 (4th Cir.), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017).

[193] *See* Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[194] *See* Zappos.com, Inc. v. Stevens, 714 F. App'x 761 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

The first category of cases includes *Beck v. McDonald*, in which a laptop containing the personal information of 7,400 patients was stolen from a hospital.[195] The stolen personal information included names, birth dates, the last four digits of Social Security numbers, and physical descriptors (e.g., age, race, gender, height, weight).[196] The U.S. Court of Appeals for the Fourth Circuit held that the victims lacked standing under *Clapper v. Amnesty International*, another recent Supreme Court standing case that has limited plaintiffs' ability to establish Article III standing.[197] *Clapper* addresses future injuries and requires that the "threatened injury must be certainly impending to constitute injury in fact and that allegations of possible future injury are not sufficient."[198] In *Beck*, the Fourth Circuit held that the plaintiffs' future injuries and potential for identity theft were too speculative because "the mere theft of [this information], without more, cannot confer Article III standing."[199] The court also concluded that the plaintiffs' costs from purchasing credit monitoring services could not "manufacture" standing.[200]

In *Whalen v. Michaels Stores, Inc.*, the plaintiff's credit card information was likely taken in a 2014 data breach.[201] There were attempted fraudulent charges on her account, but the plaintiff canceled her card and never paid for any fraudulent charges.[202] The U.S. Court of Appeals for the Second Circuit affirmed dismissal of her complaint, noting that "she does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen."[203]

---

[195] *Beck*, 848 F.3d at 262.

[196] *Id.* at 267–68.

[197] Clapper v. Amnesty Int'l, 568 U.S. 398, 401 (2013). *Clapper*'s "certainly impending" standard is not the only way to demonstrate standing with a future injury. In 2014, the Court unanimously decided *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014), which suggests there are two alternative tests: "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur'" (citing *Clapper*, 568 U.S. at 409, 414 n.5). What's particularly odd about this conception of the future-injury standard is that "certainly impending" harms seem to be a logical subset of "substantial risk[s]." In other words, it's not clear what kind of facts would satisfy only the former without first satisfying the latter. *See, e.g.*, Marty Lederman, *Commentary:* Susan B. Anthony List, Clapper *Footnote 5, and the State of Article III Standing Doctrine*, SCOTUSBLOG (June 17, 2014, 4:34 PM), https://www.scotusblog.com/2014/06/commentary-susan-b-anthony-list-clapper-footnote-5-and-the-state-of-article-iii-standing-doctrine/ [https://perma.cc/Z27P-8SM4].

[198] *Clapper*, 568 U.S. at 409.

[199] *Beck*, 848 F.3d at 275.

[200] *Id.* at 276–77.

[201] Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).

[202] *Id.* at 89–90.

[203] *Id.* at 90.

A third breach case issued a split decision. The U.S. Court of Appeals for the Eighth Circuit found a sufficient present injury in the form of a single fraudulent charge on the credit card that one plaintiff had used at one of the defendants' stores affected by a data breach.[204] But the same panel denied standing to every other plaintiff, holding that a future injury premised on the theft of their credit card information in the same breach was insufficient for Article III.[205]

Several circuits have found standing in the context of data breaches. The U.S. Court of Appeals for the D.C. Circuit determined that *Clapper*'s future harm standard was satisfied in a case the Supreme Court declined to hear in February 2018.[206] The U.S. Court of Appeals for the Sixth Circuit also found that the potential risk of identity theft was sufficiently substantial to justify mitigation costs, and the mitigation costs were sufficient injury-in-fact to satisfy Article III.[207] The Ninth Circuit similarly concluded that an online merchant's data breach created a "substantial risk" of identity theft, thus satisfying Article III.[208] Further, in litigation over the Yahoo data breaches, a district court found that increased risk of future identity theft was sufficient to establish standing. The court noted: "Presumably, the purpose of the hack is, sooner or later, to assume those consumers' identities or to misuse Plaintiffs' [personally identifiable information] in other ways."[209]

In the second category of cases, plaintiffs have brought suit because their personally identifiable information was collected or used in a way that violates a statute. Here too, the scales tip in favor of defendants.

For example, in *Meyers v. Nicolet*, customers brought suit against a restaurant because it had failed to truncate the expiration date of the customers' credit card on transaction receipts, a violation of FACTA.[210] The U.S. Court of Appeals for the Seventh Circuit dismissed the complaint, reasoning that the plaintiffs had fallen short of *Spokeo*'s concreteness requirement, stating:

---

[204] *In re* Supervalu, Inc., 870 F.3d 763, 773–74 (8th Cir. 2017).

[205] *See id.* at 769–71.

[206] *See Carefirst*, 865 F.3d at 620.

[207] *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("[A]lthough it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. . . . [I]t would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security." (citation omitted)); *see also* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 689–90 (7th Cir. 2015) (finding standing following a merchant's data breach).

[208] *See* Stevens v. Zappos.com, Inc., 888 F.3d 1020, 1023–29 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

[209] *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (internal quotation marks and citations omitted).

[210] Meyers v. Nicolet, 843 F.3d 724 (7th Cir. 2016).

"[I]t is hard to imagine how the expiration date's presence could have increased the risk that [plaintiffs'] identity would be compromised."[211]

In *Hancock v. Urban Outfitters, Inc.*, customers alleged that retailers had violated two consumer protection statutes by requesting customers' zip codes in connection with credit card purchases.[212] The D.C. Circuit held that the plaintiffs' "naked assertion that a zip code was requested and recorded without any concrete consequence" did not satisfy the requirements of *Spokeo*.[213]

The same was true in *Braitberg v. Charter Communications, Inc.*[214] There, plaintiffs sued their former cable television provider for retaining their addresses, telephone numbers, and Social Security numbers.[215] The plaintiffs argued that retaining the information violated a provision of federal law that requires cable providers to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected."[216] The Eighth Circuit dismissed the case, holding that the allegation was of a "bare procedural violation, divorced from any concrete harm."[217] The Seventh Circuit came to the same conclusion a few months later.[218]

In contrast, the U.S. Court of Appeals for the Third Circuit ruled in favor of the plaintiffs' statutory violation claim in 2017's *In re Horizon Healthcare Services Inc. Data Breach Litigation*.[219] There, two laptops containing unencrypted personal information of 839,000 people were stolen from a health insurer.[220] The plaintiffs brought a class action suit under the FCRA, alleging that the insurer had illegally furnished their personal information and that the company violated the FCRA by failing to adopt reasonable procedures to protect their information.[221] The court reasoned that "with the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm."[222] The court, reiterating a past circuit precedent,

---

[211] *Id.* at 736–38; *see also* Kirchein v. Pet Supermarket, Inc., 297 F. Supp. 3d 1354 (S.D. Fla. 2018) (dismissing suit against a retailer for printing the first six and last four digits of his credit card number on a transaction receipt in violation of FACTA).

[212] Hancock v. Urban Outfitters, Inc., 830 F.3d 511 (D.C. Cir. 2016).

[213] *Id.* at 514.

[214] Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 (8th Cir. 2016).

[215] *Id.* at 927.

[216] 47 U.S.C. § 551(e) (2012).

[217] *Braitberg*, 836 F.3d at 930–31.

[218] *See* Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017).

[219] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017).

[220] *Id.* at 630.

[221] *Id.* at 631.

[222] *Id.* at 639.

noted that "unauthorized disclosures of information have long been seen as injurious."[223]

After *Spokeo*, some lower courts have relied on analogies to common-law privacy torts in the few cases where plaintiffs have established Article III standing.[224] For example, the Ninth Circuit—on remand in *Spokeo* itself—held that, "[e]ven if there are differences between FCRA's cause of action and those recognized at common law, the relevant point is that Congress has chosen to protect against a harm that is at least closely similar *in kind* to others that have traditionally served as the basis for a lawsuit."[225]

The Court declined an opportunity to refine the post-*Spokeo* standing inquiry during the October 2018 Term. The Court initially granted the case, *Frank v. Gaos*, to address a *cy pres* settlement under the Stored Communications Act[226] but requested supplemental briefing on Article III standing after oral argument.[227] In a per curiam opinion, the Court vacated and remanded the case and instructed the lower courts to consider the standing issue in the first instance.[228]

4. Statutory Standing in State Court

The takeaway is that standing in federal court is uncertain and inconsistent, particularly when it comes to information-related harms. But a remedy for information misuse is not limited to federal law; about half the states have explicitly declined to follow *Lujan* and Proposition B.[229] "To say that Article III's limitations on the 'federal judicial power' apply only in federal

---

[223] *Id.* at 638 (quoting *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 274 (3d Cir. 2016)) (internal quotation marks omitted) (emphasis omitted).

[224] *See* Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2460 (2018).

[225] Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 931 (2018).

[226] *See* Frank v. Gaos, 869 F.3d 737 (9th Cir. 2017), *cert. granted*, 138 S. Ct. 1697 (2018).

[227] *See* U.S. SUPREME COURT, ORDERS IN PENDING CASES (Nov. 6, 2018), https://www.supremecourt.gov/orders/courtorders/110618zr_6537.pdf [https://perma.cc/LQ5F-FU6B] (ordering supplemental briefing to address Article III standing in a case about a *cy pres* settlement reached over alleged violations of the Stored Communications Act); *see also* Transcript of Oral Argument at 15–21, 28–33, 45–46, Frank v. Gaos, No. 17-961 (Oct. 31, 2018), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2018/17-961_j42k.pdf [https://perma.cc/TYS7-PVC2] (discussing Article III standing); Brief for the United States as Amicus Curiae Supporting Neither Party at 11–15, Frank v. Gaos, No. 17-961 (July 16, 2018), https://www.supremecourt.gov/DocketPDF/17/17-961/54428/20180716192524453_17-961%20nsacUnitedStates.pdf [https://perma.cc/8SA9-HR5R] (arguing that there's no injury-in-fact under *Spokeo*).

[228] Frank v. Gaos, 139 S. Ct. 1041 (2019) (per curiam); *see also In re* Google Referrer Header Privacy Litig., 87 F. Supp. 3d 1122 (N.D. Cal. 2015).

[229] *See* Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC. & NAT. RESOURCES L. 349, 349 (2016).

court is to state a tautology. . . . The point is therefore worth stressing: federal standing doctrine has no bearing in state court."[230]

The differential treatment of standing in state and federal court can have odd effects.[231] Sometimes federal courts are unable to consider diversity cases because state law provides for a cause of action that does not satisfy Article III.

For example, in *Lee v. American National Insurance Co.*, Lee—a resident of California—sued a Texas insurance company in California state court under California's unfair business practice statute.[232] California law, at the relevant time, conferred standing on any person acting in the public interest to sue a business engaged in an unfair business practice;[233] the plaintiff had not purchased insurance from the defendant or been harmed in any other way.[234] The defendant removed the case to federal court, and the Ninth Circuit concluded that the plaintiff lacked standing in federal court to pursue his unfair business claim, noting: "Lee's standing-deficient claims will have to be disposed of in some manner on remand to the district court. . . . [T]here should be no obstacle to Lee's refiling them in state court, where he apparently has a viable cause of action which is not time-barred."[235]

A related issue recently arose in the Seventh Circuit in *Collier v. SP Plus Corp.*[236] There, customers brought a putative class action in Illinois state court against the operator of an airport parking facility, alleging that their receipts included payment card expiration dates in violation of FACTA.[237]

---

[230] *See* Trevor W. Morrison, *Private Attorneys General and the First Amendment*, 103 MICH. L. REV. 589, 629 (2005).

[231] *See* F. Andrew Hessick, *Standing in Diversity*, 65 ALA. L. REV. 417, 427 (2013) (arguing that standing should, for *Erie* purposes, be considered substantive law that federal courts apply in diversity cases); *cf.* William A. Fletcher, *The "Case or Controversy" Requirement in State Court Adjudication of Federal Questions*, 78 CAL. L. REV. 263 (1990) (arguing against state courts adjudicating federal questions when federal courts could not entertain the same claim because of a standing defect).

[232] Lee v. Am. Nat'l Ins. Co., 260 F.3d 997 (9th Cir. 2011).

[233] *See* CAL. BUS. & PROF. CODE § 17204 (2018) (authorizing civil action to enforce Unfair Business Practices Act, CAL. BUS. & PROF. CODE § 17200 (2018), by "any person acting for the interests of itself, its members, or the general public") (since amended).

[234] *See Lee*, 260 F.3d at 999 ("[T]he district court explained that because Lee had not purchased an ANTEX policy, he could not demonstrate that he had suffered an actual injury and therefore could not establish standing to bring suit in federal court.").

[235] *Id.* at 1006; *see also* Coyne v. Am. Tobacco Co., 183 F.3d 488 (6th Cir. 1999) (remanding a diversity case to state court where plaintiffs' state-law restitution claim was premised on state law permitting taxpayer standing).

[236] *See* Collier v. SP Plus Corp., 889 F.3d 894 (7th Cir. 2018) (per curiam); *see also* Skadden, Arps, Slate, Meagher & Flom LLP, *The Class Action Chronicle*, Winter 2016, https://www.skadden.com/insights/publications/2017/01/the-class-action-chronicle--winter-2016 [https://perma.cc/TC2X-28JZ] (discussing federal law class actions remanded to state court after *Spokeo*).

[237] *See Collier*, 889 F.3d at 895–96.

The defendant removed the case to federal court pursuant to federal question jurisdiction. A week later, the defendant moved to dismiss the case, arguing that the federal court lacked Article III jurisdiction because the plaintiffs failed to allege a sufficiently concrete injury-in-fact under *Spokeo*.[238] The plaintiffs agreed that the federal court lacked jurisdiction and sought remand to state court.[239] The district court sided with the defendant and dismissed the case with prejudice, but the Seventh Circuit reversed, explaining that the remand statute "required the district court to remand this case to state court, because it does not satisfy Article III's requirements."[240]

* * *

In sum, because any effort to provide a remedy for information misuse is certain to encounter significant constitutional standing problems under federal law, this proposed private enforcement remedy should be adopted only at the state level. To be sure, there are logistical hurdles to the state-law approach, such as litigating removal and remand, claim splitting, and preemption.[241] But on the whole, the uncertainty wrought by *Lujan* and *Spokeo* will continue to corrode the deterrence and incentive-shifting effects of any privately enforceable remedy. State law provides a viable alternative.

B. Why Breach of Fiduciary Duty?

The private enforcement remedy should impose a fiduciary duty on entities that collect and use information about users. In this Section, I articulate some deficiencies with other regulatory approaches, describe the particulars of a tort for breach of an information fiduciary's duty, explain why this structure minimizes First Amendment objections, and argue that imposing a fiduciary duty to users is a desirable and elegant counterbalance to the current disequilibrium.[242]

---

[238] *See id.*

[239] *See id.* at 895 ("This case presents an unusual circumstance: both parties insist that the plaintiffs lack Article III standing to sue. . . . [The plaintiffs] responded by moving to remand to state court, arguing that it was [the defendant's] responsibility to establish subject-matter jurisdiction and that, without it, 28 U.S.C. § 1447(c) required the district court to return their case to state court.").

[240] *Id.* at 897 (citing, *inter alia*, 28 U.S.C. § 1447(c); Smith v. Wis. Dep't of Agric., Trade & Consumer Prot., 23 F.3d 1134, 1142 (7th Cir. 1994); Me. Ass'n of Interdependent Neighborhoods v. Comm'r, Me. Dep't of Human Servs., 876 F.2d 1051, 1053–54 (1st Cir. 1989). *But see* Paul J. Katz, *Standing in Good Stead: State Courts, Federal Standing Doctrine, and the Reverse-*Erie *Analysis*, 99 NW. U. L. REV. 1315, 1352 (2005) ("[I]t seems unreasonable that the Constitution would allow Congress to utilize state courts to enforce statutory directives where federal courts cannot.").

[241] The advantages of and challenges to this approach are discussed in more detail in Part V, *infra*.

[242] *See infra* notes 243–291 and accompanying text.

1. The Inadequacy of Public Enforcement and Contract Law

Enforcement of information privacy through a centralized public regulator has many drawbacks. For one, it may raise serious First Amendment questions.[243] The GDPR's "right to erasure," for example, probably cannot be enforced in the United States, at least with regard to true information.[244] Second, the FTC's experience to date is clearly inadequate to meaningfully deter information misuse.

Some scholars have proposed that privacy rights should be regulated through contract.[245] For example, Eugene Volokh has advocated for a contract model of privacy to ameliorate First Amendment concerns.[246] He argues that, because agreements not to disclose are generally enforceable,[247] contracts provide an avenue for private parties to enforce speech limitations that the government could not achieve through direct regulation.[248] The practical effect would be that any representations a company makes about its information privacy practices in its terms of service would be strictly enforceable. Because of the inherent limits of regulation through terms of service, Volokh also advocates broadly using implied contracts for privacy that are based on custom, course of dealing, reasonable expectations, and other relevant factors.[249]

There are good reasons to doubt the efficacy of the contract model. The FTC's litigation strategy is instructive;[250] for a few years, the FTC pursued companies for deviations from their terms of service under a deceptive trade practice theory of liability. But the agency quickly abandoned this approach, instead favoring direct regulation of privacy practices under an unfair trade practice theory of liability.

Other scholars have explicitly highlighted the limitations of the contract model. Some have noted that the contract model doesn't accurately reflect a

---

[243] *See* Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1049 (2000).

[244] *Cf.* Muge Fazlioglu, *Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet*, 3 INT'L DATA PRIVACY L. 149, 149 (2013); *see also* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1531–33 (2015) ("[T]he right to be forgotten runs into First Amendment problems when it starts to resemble the old disclosure tort.").

[245] *See, e.g.*, Volokh, *supra* note 243, at 1051.

[246] *See id.*

[247] This includes journalists engaged in speech at the heart of the First Amendment. *See* Cohen v. Cowles Media Co., 501 U.S. 663, 668–72 (1991).

[248] Volokh, *supra* note 243, at 1057–63.

[249] *Id.* at 1057–58.

[250] *See supra* Part I.A.2.

host of federal information privacy regulations, particularly in healthcare.[251] Further, Jack Balkin has argued that, as the government uses contracts as a vehicle to impose default rules and non-waivable duties, the government is "essentially offering a tort theory of privacy protection."[252]

2. Breach of an Information Fiduciary's Duty

A tort is a civil wrong.[253] Many torts impose a duty on everyone, but not all.[254] Malpractice and breach of fiduciary duty are torts that impose a duty on a specific person or class of persons.[255] Tort law is publicly controlled and enforced by private parties.[256] This is in contrast to contract law, which is privately controlled and enforced by private parties, and in contrast to criminal law, which is publicly controlled and enforced by public parties.[257]

Many scholars have written that information misuse most elegantly fits within tort law. Some say that courts should identify a common-law tort for the misuse of personal information, which "would impose on data traders a duty to use Fair Information Practices (based on the principles of notice, choice, access, and security)."[258] Others have argued that states should use tort law to fill a remedial void that federal privacy statutes have created.[259]

Balkin has synthesized much of the foregoing—First Amendment concerns, the limits of the contract model, and the advantages of tort.[260] In doing so, he has proposed imposing a fiduciary duty on entities that collect, analyze, use, disclose, or sell personally identifiable information.[261] He explains: "My central point is that certain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships*

---

[251] *See* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1159, 1565–66 (2000).

[252] Balkin, *supra* note 9, at 1204; *see also id.* at 1199–1205.

[253] BRYAN A. GARNER, GARNER'S DICTIONARY OF LEGAL USAGE 898 (3d ed. 2011).

[254] *See id.* (defining a tort as "the breach of a duty that law imposes on everyone" but noting that this definition "is barely adequate because it is perhaps impossible to give an exact definition [and] . . . because there is no common set of traits that every tort possesses").

[255] *See, e.g.*, Meyers v. Livingston, Adler, Pulda, Meiklejohn & Kelly, P.C., 87 A.3d 534 (Conn. 2014) (concluding that breach of fiduciary duty sounded in tort, rather than contract).

[256] Christian Turner, *Law's Public/Private Structure*, 39 FLA. ST. U. L. REV. 1003, 1010–13 (2012).

[257] *See id.*

[258] *See, e.g.*, Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 172–73 (2007).

[259] *See, e.g.*, De Armond, *supra* note 150, at 1.

[260] *See Balkin*, *supra* note 9.

[261] *Id.* at 1205–09.

that produce them."[262] Here is how Balkin defines an information fiduciary and the scope of one's duties:

> An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship. . . . [P]rofessionals have duties to use the information they obtain about their clients for the client's benefit and not to use the information to the client's disadvantage.[263]

Balkin's approach is sound. Other scholars have recognized the strengths of this approach.[264] Accordingly, one or more states should enact a statute that creates a tort cause of action for breach of an information fiduciary's duties.

3. Protection Against a Weaponized First Amendment

An aggressive interpretation of the First Amendment presents the greatest existential threat to the proposed information security regulatory regime.

The Supreme Court's 2011 decision in *Sorrell v. IMS Health, Inc.* presents the most foreboding precedent for any information security regulation, and it has been accurately described as the "original sin" of First Amendment overreach.[265]

Sorrell concerned a Vermont law that prohibited pharmacies from selling data about physicians' prescribing habits to pharmaceutical companies.[266] Pharmaceutical companies use this data to tailor their physician-targeted marketing campaigns, hoping to persuade physicians to prescribe a pharmaceutical company's new and expensive drugs more frequently; this process is called "detailing."[267] When it enacted this prohibition, Vermont cited several government interests, including how detailing misleads physicians, increases

---

[262] *Id.* at 1205.

[263] *Id.* at 1209.

[264] *See, e.g.*, DeLuca, *supra* note 224, at 2468; Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 628 (2018), https://www.yalelawjournal.org/pdf/Solow-Niederman_qthw8784.pdf [https://perma.cc/LSR8-32G2].

[265] Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011); *The Hard Drive Has Always Been the Enemy: Episode 177*, ORAL ARGUMENT (Aug. 7, 2018), https://oralargument.org/177 [https://perma.cc/7G5B-9A3L].

[266] *Sorrell*, 564 U.S. at 557. The information is not purchased directly by pharmaceutical companies; instead, an intermediary—which the Court calls a "data miner"—purchases the information from the pharmacies and creates reports about physicians' prescribing habits, which the miners then lease to the pharmaceutical companies. *See generally id.* at 558.

[267] *See id.* at 557–59.

the cost of healthcare and health insurance, and "encourages hasty and excessive reliance on brand-name drugs."[268]

Writing for a six-justice majority, Justice Kennedy explained that the Vermont law was inconsistent with the First Amendment, and the Court struck it down.[269] Justice Kennedy first concluded that the Vermont law was a content- and speaker-based restriction on protected expression and thus subjected the law to heightened judicial scrutiny.[270] He rejected the argument that the law was merely a commercial regulation, concluding that the law "impose[d] more than an incidental burden on protected expression."[271] The Court also broadly defined protected speech to include almost any "creation and dissemination of information."[272] Straining credulity, Justice Kennedy analogized the Vermont law to "a law prohibiting trade magazines from purchasing or using ink."[273]

The majority also dramatically narrowed the distinction between viewpoint-discriminatory strict scrutiny and heightened scrutiny under the commercial speech doctrine. The majority wrote: "To sustain the targeted, content-based burden [the Vermont law] imposes on protected expression, the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest."[274] Although the majority conceded that the state's interests were substantial, the Court invalidated the law on tailoring grounds.[275]

Sorrell is an ominous sign for any information security regulation for at least three distinct reasons. The first is the Court's definition of an "incidental burden" on protected expression. In *Sorrell*, the Court rejected the argument that the information—collected pursuant to a government mandate—was akin to a commodity. The state had argued that the data was rather unlike the core expression at the center of the First Amendment's protection. The Court flatly rejected the suggestion that different kinds of information should be treated differently. Adhering to this expansive definition would invalidate almost any conceivable government regulation that touches or concerns speech.[276]

Second, the Court explicitly held that a business model premised on the collection, collation, retention, and exploitation of data was core protected

---

[268] *See id.* at 561.
[269] *See id.* at 602–03.
[270] *See id.* at 552.
[271] *See id.* at 567.
[272] *Id.* at 553.
[273] *Id.*
[274] *Id.* at 571.
[275] *See id.* at 572–80.
[276] *Cf.* Janus v. AFSCME, 138 S. Ct. 2448, 2487 (2018) (Kagan, J., dissenting) (listing, *inter alia*, securities regulation).

expression. This means that any direct regulation of businesses that traffic in personal information will likely be subjected to something approaching strict-in-theory and fatal-in-fact scrutiny. And third, the Court's erasure of the distinction between heightened scrutiny of commercial speech and true strict scrutiny is particularly disquieting.

The information fiduciary frame provides perhaps the strongest possible footing for users to reassert control over how businesses use—and misuse—their information. Balkin argues that, when it comes to information obtained and disseminated within commercial and economic activities, the social context of the information collection and dissemination governs whether the information receives First Amendment protection. He notes: "[T]he speech that occurs in fiduciary relationships is not public discourse. When law regulates professional relationships with clients in fields like law or medicine, it often regulates the way that professionals speak to clients and requires that they not use client information against the client's interest."[277] For that reason, "when a fiduciary communicates private information about a client to the public, the communication does not receive standard First Amendment protection, unless the dependent person . . . permits the information to enter public discourse."[278]

Balkin illustrates this principle through a hypothetical whereby a gynecologist creates an art installation called "Crazy Stuff My Patients Say," which contains actual information conveyed by patients in the course of receiving medical care.[279] The art installation "does not receive full First Amendment protection even though it takes the form of contemporary art," because "[i]t uses information obtained in a fiduciary relationship without permission from the affected patients."[280] Just as you can sue the gynecologist for failing to protect your sensitive information, you can sue the person who misuses your data. And, critically, you can also sue the person who failed to appropriately secure your data. Balkin argues that "the doctor has a fiduciary duty to ensure that the privacy protections run with the data,"[281] meaning that you do not need separate contracts with every person who handles the information because "it is the fiduciary's job to ensure that [your] privacy is protected."[282]

---

[277] Balkin, *supra* note 9, at 1216.
[278] *Id.* at 1219.
[279] *Id.* at 1209–10.
[280] *Id.* at 1219.
[281] *Id.* at 1220.
[282] *Id.*

Although compelling, it would be a mistake to suggest that First Amendment issues are easy to resolve and will necessarily favor users over businesses. In recent years we have seen numerous legal challenges to novel regulatory regimes that the Supreme Court divisively resolved,[283] and the First Amendment rights of business is ascendant among the Court's conservative majority.[284]

As Justice Kagan has argued, a majority of the Court has "turn[ed] the First Amendment into a sword, and [is] using it against workaday economic and regulatory policy."[285] Although Justice Kagan was writing in the context of public sector union fees, her warning applies with equal force to putative information security regulation. She explains: "Speech is everywhere—a part of every human activity (employment, health care, securities trading, you name it). For that reason, almost all economic and regulatory policy affects or touches speech. So the majority's road runs long. And at every stop are black-robed rulers overriding citizens' choices."[286]

4. Balancing Fiduciaries' Interests

The information fiduciary duty approach has many advantages. Imposing a fiduciary duty to users would provide a desirable and elegant counterbalance to the current incentives, which induce underinvestment in security and provoke excessive information retention. As discussed in Part II, shareholders exert persistent downward pressure on investment in information security. Instituting a fiduciary duty between the company and the users will counteract the unchecked interests of shareholders.

To put a finer point on it, underinvesting in security and retaining excessive data are often perfectly rational decisions in the current environment. Yahoo provides an instructive example of the former. In 2010, Chinese military hackers infiltrated several Silicon Valley technology companies, including Google and Yahoo.[287] Following these intrusions, the two companies took starkly different paths: Google doubled down on security, hiring hundreds of well-compensated security engineers, investing hundreds of millions of dollars in security, and adopting a new internal motto—"Never Again."[288] Yahoo, on the other hand, was in the midst of staging a corporate turnaround,

---

[283] *See, e.g.*, King v. Burwell, 135 S. Ct. 2480 (2015); Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519 (2012).

[284] *See, e.g.*, Burwell v. Hobby Lobby Stores, Inc., 573 U.S. 682 (2014); Citizens United v. FEC, 558 U.S. 310 (2010).

[285] *Janus*, 138 S. Ct. at 2502 (Kagan, J., dissenting) (citing, *inter alia*, *Sorrell*, 564 U.S. 552).

[286] *Id.*

[287] *See* Perlroth & Goel, *supra* note 122.

[288] *Id.*

and the company did not meaningfully invest in cybersecurity—officers even stigmatized security-minded employees by dubbing them the "Paranoids."[289]

These decisions are worthy of criticism, but they were nonetheless rational choices at the time they were made: "Specifically, Yahoo may convincingly argue [in a shareholder derivative suit] that the corporate turnaround it was attempting to stage in the midst of the breach was inherently a risky proposition."[290] Although we may tolerate the ramifications of that risky proposition for shareholders, we shouldn't demand that uninformed users do the same. If anything, shareholders have assumed the risk of information misuse costs to a far greater degree than users of a company's electronic services.

Sometimes playing fast and loose with information security is profitable—or, worse, is perceived to be potentially profitable.[291] Imposing a fiduciary duty between users and companies will help defeat this perverse incentive. Instead of allowing companies to commoditize users' information for shareholder benefit, corporate officers will need to balance competing fiduciary interests—how to maximize profit without betraying users.

* * *

In sum, regulating information security faces many legal hurdles. Imposing a fiduciary duty on companies that collect and retain users' personally identifiable information overcomes several of these hurdles and also provides a counterbalance to unchecked shareholder excesses.

C. Why Strict Liability?

An information fiduciary duty is a good start. But it, alone, is unlikely to sufficiently shift corporate incentives to invest heavily in information security. To give this tort some teeth, the law should impose strict liability for breach of an information fiduciary's duty. In this Section, I identify the shortcomings of a negligence regime, make an affirmative case for strict liability, and examine the arguments against strict liability.[292]

There are significant hurdles to successfully applying negligence law to information misuse. "[P]laintiffs so far have had little success in obtaining

---

[289] *Id.*

[290] Trautman & Ormerod, *supra* note 34, at 1282.

[291] The perception that underinvestment in information security is a potentially profitable strategy is—from the perspective of reshaping incentives—somewhat worse than the reality.

[292] *See infra* notes 293–307 and accompanying text.

tort recovery for . . . instances of identity theft."[293] Because negligence "requires a court to resolve apparently insurmountable issues pertaining to the elements of duty, breach, and compensable harm . . . the black-letter rules would seem to either bar the tort claim or make it extremely difficult for victims of identity theft to recover for their losses."[294]

The rationales for strict liability in products cases apply with even more force to informational harms: "[V]ictims of identity theft would have to prove what reasonable care requires within a technologically complex and constantly evolving environment, an evidentiary burden comparable to, if not greater than, the burden faced by a consumer trying to prove that a product manufacturer failed to adopt reasonable quality-control measures."[295]

Several scholars have argued that data breaches and other common types of information misuse should be evaluated under a strict liability regime.[296]

There are two primary reasons the law ever turns to strict liability. First, a negligence standard fails when there is difficulty attributing liability and difficulty recovering damages, which result "from the multiplicity of actors and the complexity of their interconnected relationships."[297]

Second, a strict liability standard ensures that liability for harms is assigned to the party or parties best able to bear it.[298] Under a negligence standard, the law assumes the parties are relatively symmetrical—that "[both] parties bear, and are able to bear, comparable responsibility for preventing or accepting the risk of harm."[299] We employ strict liability in the context of ultrahazardous activities and products liability because they present "risks that would be unreasonably, or impossibly, costly for individuals to detect."[300]

Both reasons weigh in favor of applying strict liability to information misuse. Cybersecurity is sufficiently complex that attributing liability under a negligence regime is effectively impossible.[301] And it is similarly absurd to suggest that users are capable of bearing cybersecurity risks. Companies hold

---

[293] Mark A. Geistfeld, *Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability*, 66 DEPAUL L. REV. 385, 387 (2017).

[294] *Id.*

[295] *Id.* at 404.

[296] *See, e.g.*, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007); Hurwitz, *supra* note 137, at 1520–30.

[297] Hurwitz, *supra* note 137, at 1526.

[298] *Id.* at 1525.

[299] *Id.*

[300] *Id.*

[301] *See* Geistfeld, *supra* note 293, at 387.

themselves out as being trustworthy caretakers of your information,[302] and there is almost nothing a user can do to corroborate those representations or interrogate the sufficiency of a company's information security practices.[303]

To be sure, strict liability has its own challenges. For one, strict liability, alone, does nothing to resolve the question of damages.[304] This is one of the reasons that a state should enact a statutorily prescribed schedule of damages.

A second issue concerns who should be subject to strict liability. Because cybersecurity is a complicated web of interconnected actors—any one of which could be primarily at fault for information misuse[305]—the question is: which actors should be covered by the statute and thus subject to strict liability?

At the very least, consumer-facing businesses that collect information from consumers should be covered because they "present a near-classic case in which strict liability is appropriate," and any information security strict liability regime "should be designed to apply only to those firms where principles of ordinary negligence or contract law do not sufficiently protect parties from security related risks."[306] Data traffickers (or data "brokers") also provide a perfect example of the attributes of the kind of parties that should be subject to strict liability.[307] Several states already have statutes that address what constitutes a "covered entity" for purposes of their breach notification and information security statutes, and in many cases these definitions suffice for a starting point for assigning strict liability.

---

[302] *See* Balkin, *supra* note 9, at 1223 ("By presenting themselves as trustworthy collectors and keepers of our individual data, and by emphasizing that, for reasons of security and competitiveness, they cannot be fully transparent, digital organizations induce relations of trust from us, so that we will continue to use their services."); *see also* Mark Zuckerberg, FACEBOOK (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071 [https://perma.cc/ZYW4-5Q7D] ("We have a responsibility to protect your data, and if we can't then we don't deserve to serve you.").

[303] *See* Balkin, *supra* note 9, at 1222 ("Online service providers have lots of information about us, and we have very little information about them or what they can do with the information they have collected. It is easy for online service providers to monitor what we do, especially as they collect increasing amounts (and kinds) of data about us. But it is generally very difficult for us to monitor their operations and prevent them from acting against our interests or otherwise betraying our trust.").

[304] *See* Hurwitz, *supra* note 137, at 1529.

[305] *See, e.g.*, Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 14, 2014), https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data [https://perma.cc/4KGR-VZG8] (explaining that a third-party vendor was responsible for introducing malware into Target's system but that Target itself failed to heed multiple alarms to avert or blunt the breach).

[306] Hurwitz, *supra* note 137, at 1530.

[307] *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 665 (2019).

In short, if a business model is premised on the company collecting, retaining, processing, selling, or sharing users' information, the statute should presume the company is covered and thus subject to strict liability.

D. Why Nominal Damages?

The private enforcement remedy should impose only nominal damages (and reasonable attorney's fees) for strict liability. But as a defendant becomes more culpable for information misuse, the penalty should ratchet up. Below, I explain why using the so-called private attorney general doctrine is a sound approach to enforcing remedies for information misuse.[308]

The private attorney general doctrine allows private citizens to enforce public rights, in contrast to enforcement by a public regulator.[309] The private attorney general doctrine is thus a partial exception to the American rule that each party usually covers its own legal expenses.[310] Granting attorney's fees to successful litigants incentivizes these suits: In the classic case, a party brings suit to enforce a right that would otherwise not be enforced.[311] Hence, by granting attorney's fees, "a court applying the doctrine is in effect reordering public policy priorities established by the political process through the creation of judicial incentives for the enforcement of such unenforced rights."[312]

Congress has used the private attorney general doctrine in several contexts, such as in the Civil Rights Act of 1964[313] and in the Americans with Disabilities Act.[314] Over time, however, federal courts have undermined the efficacy of this regulatory regime by concluding that plaintiffs who receive

---

[308] *See infra* notes 309–318 and accompanying text.

[309] *See* Carl Cheng, *Important Rights and the Private Attorney General Doctrine*, 73 CAL. L. REV. 1929 (1985).

[310] *Id.* at 1929 n.1.

[311] *See, e.g.*, Kenneth Sanney, Note, *Cyberjacking, Mousetrapping, and the FTC Act: Are Federal Consumer Protection Laws Helping or Hurting Online Consumers?*, 3 VAND. J. ENT. L. & PRAC. 221, 231–32 (2001) ("[T]he selective, slow, and often cumbersome FTC policies of enforcement do not provide adequate protection for consumers in this new marketplace. . . . Availability of private enforcement would give consumers the opportunity . . . to pursue acts of deception and fraud on the Internet, while simultaneously deterring, and imposing responsibility for, bad acts by online businesses.").

[312] Cheng, *supra* note 309, at 1929.

[313] *See* Newman v. Piggie Park Enters., Inc., 390 U.S. 400, 402 (1968) (per curiam) ("When a plaintiff brings an action under [Title II of the Civil Rights Act of 1964], he cannot recover damages. If he obtains an injunction, he does so not for himself alone but also as a 'private attorney general,' vindicating a policy that Congress considered of the highest priority."); Alan Schoenfeld, *Attorney's Fees "R" Us: The Significant Public Purpose Doctrine Comes to State Court*, 23 YALE L. & POL'Y REV. 601, 601–02 (2005).

[314] *See* 28 C.F.R. § 36.501 (2012) (authorizing private ADA suits); *id.* § 36.505 (authorizing prevailing party attorney's fees).

nominal damages are not entitled to attorney's fees.[315] This hostility in the federal courts towards the private attorney general doctrine is another reason to adopt this proposal at the state level.

Pairing the private attorney general doctrine with robust breach notification is a powerful way to shift incentives. Any person who receives notice of information misuse should be empowered to bring suit against the offending organization. Binding these two rights together—the right to receive notice and the right to bring a private suit—helps overcome one of the biggest obstacles to information misuse litigation: attributing liability. (Strict liability helps overcome the other big obstacle: proving and recovering damages.)

The proposed penalty schedule should apply to both the information misuse itself and compliance with breach notification requirements. Strict adherence to breach notification has largely failed to date because there is no meaningful mechanism to require companies' compliance.[316] Under the GDPR, for example, companies that fail to notify affected persons about a data breach are subject to fines of ten million euros or two percent of annual revenue, whichever is higher.[317]

There are three primary reasons for using the penalty schedule proposed above in Part III.B. First, it provides the opportunity for discovery. By requiring companies to notify users about the breach, providing a private cause of action, and imposing strict liability, users will be empowered to bring suit against companies that have misused their data. Upon bringing suit, these private attorneys general will have the authority to conduct discovery to determine whether an organization was negligent, reckless, or worse. In other words, structuring the remedy in this way requires companies that misuse users' information to finance an outside investigation into their information security failures.

---

[315] *See, e.g.*, Lawrence D. Rosenthal, *Adding Insult to* No *Injury: The Denial of Attorney's Fees to "Victorious" Employment Discrimination and Other Civil Rights Plaintiffs*, 37 FLA. ST. U. L. REV. 49, 52 (2009) ("Since [*Farrar v. Hobby*, 506 U.S. 103 (1992)], most courts have determined that plaintiffs who receive only nominal damages are not entitled to attorney's fees.").

[316] *See, e.g.*, Trautman & Ormerod, *supra* note 34, at 1268–70 (explaining that Yahoo's security team—and likely also senior management—knew about the breaches in December 2014 but didn't notify the public until September 2016); Karen Freifeld & John McCrank, *N.Y. Regulator Subpoenas Equifax Over Massive Breach*, REUTERS (Sept. 27, 2017), https://www.reuters.com/article/us-equifax-cyber-new-york-exclusive/exclusive-n-y-regulator-subpoenas-equifax-over-massive-breach-idUSKCN1C22LU [https://perma.cc/TJV5-VB93] (mentioning that it took Equifax forty-one days to notify the public about a data breach that compromised extremely sensitive information about more than 140 million Americans); Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html [https://perma.cc/KEP6-9GA4] (noting that Uber's attempts to pay hackers a ransom to delete stolen data likely violated FTC rules and California breach notification laws).

[317] *See* GDPR, *supra* note 103, Art. 83(4).

Second, the law should shift incentives without being unduly punitive. If a company has not been negligent or worse, the company may only be liable for nominal damages and attorney's fees. This thus prompts a company to finance an investigation; if no additional wrongdoing is found, the company may not be liable for anything other than the costs of the investigation (assuming the cost of the investigation is sufficient to meaningfully deter future information misuse).[318]

Third, the scheme prevents a windfall for the attorneys that bring suit. Because of contingent fee arrangements, there may be an inequitable windfall for the named plaintiffs' lawyers to grant them both fees and a third of compensatory damages if the company has not been negligent. Accordingly, if a company has not been negligent (or worse), the private attorney general should be paid a reasonable fee, and uncovering greater wrongdoing thus has its own financial incentive. And requiring that companies remit penalties to the state treasury also enables deterrence without an undue windfall.

V. ADVANTAGES AND CHALLENGES

The proposed private enforcement remedy has both advantages and drawbacks. Part III described the proposed right and remedy.[319] Part IV provided the rationales for the remedy's four core features.[320] Section A of this Part articulates normative reasons for adopting the proposal.[321] Section B then highlights some particular challenges to the proposed approach.[322]

A. Advantages of a Private Enforcement Remedy

There are five primary benefits of the private enforcement remedy—furthering three primary goals and two practical advantages.

1. Primary Goals

The private enforcement remedy will further three primary goals: incentivizing more investment in information security, disincentivizing excessive data retention, and bolstering the market for cybersecurity insurance.

The first primary benefit is that the remedy ensures that companies that misuse users' information will be held liable. Companies will thus have greater incentive to invest in information security and to prevent information misuse.

---

[318] *See supra* note 152 and accompanying text.
[319] *See supra* notes 139–155 and accompanying text.
[320] *See supra* notes 156–318 and accompanying text.
[321] *See infra* notes 323–340 and accompanying text.
[322] *See infra* notes 342–348 and accompanying text.

More specifically, adopting this proposal will help address the three reasons for persistent too-little security disequilibrium articulated in Part II.B. First, information misuse persists because it is currently an externality—users pay the costs of the company's information security failures. By making liability a certainty, the law would begin internalizing these costs. Adopting the remedy would shift these costs more directly onto the misusing company.

Second, information misuse persists because of variability of marginal costs. I address that below in the context of cybersecurity insurance. Third, information misuse persists because of information imperfection—the idea that a company, ex ante, has little way to know how much it should invest in cybersecurity because it cannot concretely forecast the costs of an information misuse incident. The remedy combats this problem by promoting more perfect information. The proposal will help clarify that, if a company misuses its users' information, the company will at least owe nominal damages and attorney's fees. This clarity will allow the company to make more informed decisions about investing in information security.

The second primary benefit is that the remedy will impose some actual costs on excessive information retention. Disincentivizing information retention is an unbridled benefit of this approach.

The law must answer two questions about information security regulation: "When is it legal to gather that information? And once it is gathered, how long may it be retained?"[323] The answer to those questions right now—with a few exceptions—is that "anything may be gathered by anyone and kept forever."[324] But, as briefly alluded to earlier, direct regulation of information expungement is likely to face constitutional challenges.[325] By raising the costs of information retention, the proposed enforcement remedy will create—for the first time—an incentive for companies to destroy, rather than retain, every byte of user data. This remedial scheme will thus promote improvements in both information security and digital privacy, accomplishing the latter by raising the transaction costs of retaining excessive user information.[326]

The ongoing debacles at Facebook have laid bare the absurdity of the digital advertising ecosystem. Although the Cambridge Analytica incident

---

[323] Ian J. Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2916 (2018).

[324] *Id.*

[325] *See supra* Part IV.B.

[326] *Cf.* Woodrow Hartzog & Frederic D. Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 403 (2013) ("Perhaps the most obvious way to design for obscurity is to create technologies that directly produce obscurity or enable users to produce obscurity for themselves. . . . [P]rivacy settings could restrict access to various degrees and, by doing so, raise the transactional cost of finding information and making that information more obscure.").

may not technically have been a "data breach," "[i]t is something even more troubling: an all-too-natural consequence of Facebook's business model, which involves having people go to the site for social interaction, only to be quietly subjected to an enormous level of surveillance."[327] In addition to logging your every metric on nearly every Facebook product, the company collects your browsing history, purchases external information about you, and maintains shadow profiles of non-users—"an involuntary dossier from which you cannot opt out."[328]

The takeaway is this: "[T]here are now private entities that collectively aim to know every detail of our lives, from cradle to grave. They have the technology to gather it, they have the space to store it, and they have built businesses on getting it."[329] Information security policy reform should not just focus on shifting costs onto the parties who should bear them, though that would be a good start. We should also focus on why we allow this for-profit panopticon to propagate and how we can blunt its incentive structure and retard its growth.

The third primary benefit of this regulatory regime is that it will increase efficiencies and equities through shifting information misuse costs.

Many have written on the woeful state of the cybersecurity insurance industry.[330] By adopting strict liability for information misuse, the law would shift the insurance burden from users to businesses. This is normatively desirable for at least three reasons.

First, as is the case in other strict liability contexts, businesses are more capable of bearing the costs of the harm than users.[331]

Second, shifting the insurance burden to businesses is not the end of the story. Ultimately, those costs are passed back onto users in a more equitable and distributed way. How so? Businesses will now have an incentive to take out an insurance policy; the premiums of this insurance policy, then, raise the

---

[327] Zeynep Tufekci, *Facebook's Surveillance Machine*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html [https://perma.cc/59NA-MY7E].

[328] *Id.*

[329] Samuel, *supra* note 323, at 2924.

[330] Hurwitz, *supra* note 137, at 1531 ("Academics have been discussing the value of cyber insurance as a mechanism for improving the overall state of cybersecurity for over a decade, but in more recent years have lamented the insurance marketplace's failure thus far to realize this possibility." (citing Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment* (Univ. of Ill. Coll. of Law Legal Studies Research Paper No. 17-18, 2017), https://ssrn.com/abstract=2924854)).

[331] *See, e.g.*, Hurwitz, *supra* note 137, at 1539 ("The intuitive understanding of strict liability is that it is meant to place the burden of avoiding harm on the more sophisticated party in a relationship—generally the party with greater knowledge about the risks associated with the use of a given product or service.").

cost of the business's products.[332] "In effect, adopting a strict-liability regime is equivalent to adopting a mandate that parties have insurance against harms that may befall others with whom they interact. That is, strict liability is effectively a mandate for third-party cyber insurance."[333]

Third, as alluded to briefly above, this burden shifting helps resolve the variability of marginal costs because insurance premiums are consistent. Businesses can thus predict and plan, ex ante, how much to invest in information security with more confidence and certainty.

By imposing strict liability on information misuse, businesses are forced to insure against data breaches and other information misuse. This, alone, is good policy, because businesses are currently externalizing information misuse harms. Reality suggests the opposite should be true, because businesses are more capable of bearing these costs than users are. But there are benefits over and beyond simply shifting the costs to the appropriate party. Requiring businesses to insure against information misuse will induce them to seek someone else to underwrite this risk—namely, an insurance company. So businesses that traffic in information will all have new incentive to enter the market for insurance, which others have argued will improve the market.[334] And the net result is that the costs of information misuse will be more predictable, less variable, and more distributed across multiple actors.

2. Practical Advantages

There are two practical advantages to the proposed remedial scheme: eschewing a centralized regulator and avoiding Congress.

First, critics of the FTC and the GDPR often argue that uneven and uncertain enforcement is a problem.[335] And pro-industry critics are hardly alone

---

[332] *See id.* at 1541 ("[T]he manufacturer passes those costs along to the consumer, increasing the price of its products in order to meet the strict-liability regime's demand that it insure consumers against harm. In the products-liability market, this is exactly how strict liability works: firms purchase third-party insurance for the users of their products and incorporate the cost of this insurance into their products' prices.").

[333] *Id.*

[334] *See id.* at 1542–43 ("[A]n insurance regime inserts a layer of parties into the ecosystem—the insurers—that have an interest in systematically studying and quantifying risks, disseminating knowledge about avoiding them, and pushing for changes that reduce these risks altogether.").

[335] *See id.* at 1520 ("Another important problem with the FTC approach to cybersecurity is that it does not meaningfully inform or educate anyone about good security practices."); Shannon Togawa Mercer, *Sorting Through GDPR: What to Watch After May 25*, LAWFARE (May 25, 2018), https://www.lawfareblog.com/sorting-through-gdpr-what-watch-after-may-25 [https://perma.cc/G282-HTW7] ("[T]here is a lot of uncertainty about how the [GDPR] will be enforced. First, the regulation itself requires interpretation; its broad language will need to be narrowed and defined through use-cases. But in addition to that, the bodies dealing with early cases may not be prepared to meet their GDPR obligations.").

in their wariness of the public enforcement model. California's abrupt shift from the private-enforcement ballot measure to the public-enforcement legislation provoked sharp criticism from California's Attorney General, the office empowered to enforce the new statute.[336]

The proposed scheme would end this regulatory uncertainty and eliminate the challenges that public enforcement creates. Under this proposal, a covered entity that discovers misuse would be required to notify users about it, and a user's receipt of that notification would itself be sufficient to establish strict liability.

Congress has used this so-called private attorney general doctrine in other contexts where public enforcement is impractical. Consider, for example, the Americans with Disabilities Act. Congress provided a private right of action because it understood that the Department of Justice, alone, could not ensure widespread ADA compliance. So too here.

Second, the benefits of avoiding Congress (and federal law generally) are palpable. Congress's half-hearted attempts to update regulation of information security in the twenty-first century have failed, and the institution has largely rendered itself irrelevant.[337] If anything, Congress should be considered a threat to meaningful reform.[338] Given the powerful influence of the technology sector's lobby in Washington, any federal legislation is likely to be quite friendly to Silicon Valley and preempt more rigorous state-law regulation.[339] And that's before constitutional challenges undermine any enacted regulatory regime.

The April 2018 congressional testimony of Facebook's chief executive, Mark Zuckerberg, starkly illustrates the shortcomings of the institution. As one news report gently put it, the hearings "revealed a vast knowledge gap between Silicon Valley and the nation's capital, where lawmakers struggled

---

[336] Letter from Cal. Att'y Gen. Xavier Becerra to Cal. Assembly Member Ed Chau and Cal. Senator Robert Hertzberg (Aug. 22, 2018), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical [https://perma.cc/8BGM-XRVH].

[337] *See, e.g.*, Daniel J. Solove, *The U.S. Congress Is Not the Leader in Privacy or Data Security Law*, TEACH PRIVACY (Apr. 9, 2017), https://teachprivacy.com/us-congress-is-not-leader-privacy-security-law/ [https://perma.cc/4PQX-G638] ("Privacy and security are important policy areas, and in the past, the U.S. Congress has led. But now, sadly, Congress is becoming increasingly irrelevant, a stuffy place filled with hot air, a wasteland of increasing irrelevance. Meanwhile, it is the EU—as well as a few [U.S.] agencies, [U.S.] states, and other countries—that everyone is now paying attention to.").

[338] *See infra* Part V.B.

[339] Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html [https://perma.cc/HR8R-99X2]; Anne Weismann, *Silicon Valley Companies Lobby to Remain Unregulated*, N.Y. TIMES (Oct. 24, 2016), https://www.nytimes.com/roomfordebate/2016/10/24/silicon-valley-goes-to-washington/silicon-valley-companies-lobby-to-remain-unregulated [https://perma.cc/J8LM-JKMF].

to grasp how the technology works and which problems—misinformation, sharing of data to third parties or political biases coded into algorithms—needed to be addressed."[340] A less charitable read is that Congress lacks the technical expertise, the political will, and the institutional tools to lead in this area.

Accordingly, states should continue to lead—and they should lobby aggressively to prevent Congress's attempts to preempt state regulation.

B. Challenges for a Private Enforcement Remedy

There are three chief challenges to adopting the private enforcement remedy as proposed: the burden of litigating removal and remand, concerns over federal preemption, and lingering First Amendment concerns.[341]

The first challenge involves state law, which poses a pair of logistical hurdles, including claim splitting and the burden of litigating removal and remand. A company sued in state court for breach of fiduciary duty is likely to remove the case to federal court.[342] The federal court, however, will lack subject matter jurisdiction over the claim if it does not satisfy the *Lujan* and *Spokeo* standing requirements. Even though Article III standing is jurisdictional—so the federal court could remand *sua sponte*—plaintiffs will likely need to affirmatively argue for remand to state court.[343] It may be a burden to always litigate this issue before proceeding to discovery and the merits. The one potential upside is that, because defendants are liable for attorney's fees, defendants may realize, over time, that litigating removal and remand makes the cases more expensive and thus increases their own legal bills for essentially no benefit.

The other logistical problem is claim splitting: if a plaintiff brings any other claims alongside the breach of information fiduciary claim, the claims will likely be bifurcated and litigated separately in federal and state court. In some circumstances, only the information fiduciary claim will be remanded to state court, and thus only that claim will be subject to fee shifting.

---

[340] Cecilia Kang et al., *Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley*, N.Y. TIMES (Apr. 12, 2018), https://www.nytimes.com/2018/04/12/business/congress-facebook-regulation.html [https://perma.cc/N92W-JJ9F].

[341] *See infra* notes 342–348 and accompanying text.

[342] *See* 28 U.S.C. § 1446 (2012).

[343] *See* Lee v. Am. Nat'l Ins. Co., 260 F.3d 997, 1006 (9th Cir. 2011); Coyne v. Am. Tobacco Co., 183 F.3d 488 (6th Cir. 1999) (remanding a diversity case to state court where plaintiffs' state-law restitution claim was premised on state law permitting taxpayer standing); *see also supra* Part IV.A.4.

The second challenge involves preemption: an unavoidable consequence of creating a state law remedy is that Congress could preempt it.[344]

In August 2018, the *New York Times* reported that, in direct response to the California Consumer Privacy Act, Facebook and other technology companies had begun an aggressive lobbying campaign for federal legislation that would "put into place a kinder set of rules that would give the companies wide leeway over how personal digital information was handled."[345]

But this gamble has its own risks. Congress has repeatedly failed to enact meaningful cybersecurity legislation,[346] and even if Congress were to act, there is little to assure that covered entities will end up better off under a federal regulatory regime. In any event, House Speaker Nancy Pelosi has said that any federal legislation that preempts state law—like the California Consumer Privacy Act—is a nonstarter in the current Congress.[347]

As for the third challenge, imposing a fiduciary duty on entities that collect and retain user information insulates the remedy from some First Amendment attacks. But it would be naïve to suggest that this regulatory structure is completely immune from constitutional objection.[348] It is inevitable that, should an information fiduciary duty be enacted by statute, businesses that traffic in information will challenge the statute under the First Amendment. How, exactly, this novel regulatory regime would be resolved by the Supreme Court is uncertain and thus presents a significant potential challenge. In the end, however, the fiduciary duty provides the strongest possible argument against the First Amendment challenge.

CONCLUSION

Information security presents one of the most complex and difficult challenges of the twenty-first century. In the current state of affairs, businesses have every incentive to traffic in excessive information and have little incentive to take reasonable steps to invest in securing all that information.

---

[344] U.S. CONST. art. VI, § 1, cl. 2.

[345] Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://nyti.ms/2BPYRY2 [https://perma.cc/BRY5-RD3J].

[346] *See, e.g.*, Ed O'Keefe & Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, WASH. POST (Aug. 2, 2012), https://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html.

[347] *See* Eric Johnson, *Nancy Pelosi Says Trump's Tweets "Cheapened the Presidency"—and the Media Encourages Him*, VOX (Apr. 12, 2019), https://www.vox.com/2019/4/12/18307957/nancy-pelosi-donald-trump-twitter-tweet-cheap-freak-presidency-kara-swisher-decode-podcast-interview [https://perma.cc/NM5X-K9EP] (quoting an interview with Nancy Pelosi in which she discusses federal privacy law) ("[T]he Republicans would want preemption of state law. Well, that's just not going to happen. We in California are not going to say, 'You pass a law that weakens what we did in California.' That won't happen.").

[348] *Cf.* Janus v. AFSCME, 138 S. Ct. 2448 (2018); Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011).

Users, meanwhile, have no way to opt out of this profit-driven panopticon and have no meaningful way to vindicate their rights against companies that misuse their information.

This state of affairs is the byproduct of deliberate choices. We, as a society, have consciously decided against imposing any kind of real regulation on Silicon Valley companies, and the worst excesses of that industry have metastasized across our modern economy. Surveillance capitalism is a booming business, and we have only recently begun considering a different path.

As dispiriting as this may seem, it does not need to be this way. We can choose to stop enabling companies' externalization of informational harms, and we can choose to assign informational costs to the parties best able to bear them. Some states have already started realizing this power to choose. I believe more should follow, and the proposed remedial scheme provides a blueprint for future efforts.