Richmond Journal of Law & Technology

Volume 27 | Issue 1 Article 2

10-31-2020

Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable

Wayne Unger
Sandra Day O'Connor College of Law, Arizona State University

Richmond Journal of Law & Technology Volume XXVII, Issue 1

RECLAIMING OUR RIGHT TO PRIVACY BY HOLDING TECH. COMPANIES ACCOUNTABLE

Wayne Unger*

Cite as: Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH., no. 1, 2020.

* Founder and Chief Executive Officer, The Unger Firm LLC. Researcher, The Luminosity Lab, Arizona State University. Chief Operating Officer, MultiLucent Corporation. Juris Doctor Candidate, Sandra Day O'Connor College of Law, Arizona State University. Researcher, Disinformation Working Group, Global Security Initiative, Arizona State University. Founder and Executive Director, The Data Privacy & Technology Journal LLC. B.S., Arizona State University. All ideas, arguments, and errors are his own.

ABSTRACT

Under the present regime, data privacy and security protections are not working for individuals. Despite data privacy and security failures in recent years, Congress has not passed comprehensive legislation to protect individuals' personal information. In the absence of comprehensive federal data privacy and security legislation, states are moving at an increasing rate to enact such protections. The enforcement of these data privacy and security protections is a hotly contested issue not often discussed or explored. However, enforcement must be discussed to effectuate the substantive protections needed as more personal information is collected, used, stored, and disseminated.

Based on my professional experience in Silicon Valley and my legal and technology research, this article discusses the private right of action with respect to data privacy and security legislation, without regard to whether such legislation is enacted at a state or federal level. The purpose of this paper is to argue that if a legislature decided to enact privacy legislation, the legislation must include a limited private right of action to make the legislation effective at protecting individuals and not corporations. Only then can we reclaim our right to privacy.

I. INTRODUCTION

[1] Data privacy relates to the control, use, and dissemination of personal information (PI).[1] In recent years, federal regulators sporadically scrutinized companies for poor or deceptive data privacy practices.[2] For example, in 2019, Facebook agreed to a $5 billion fine, among other terms, in a settlement with the Federal Trade Commission (FTC) for misrepresenting to consumers (i) the extent to which consumers can control their privacy settings, (ii) the steps consumers could take to implement privacy controls, and (iii) the extent to which Facebook shares an individual's PI with third-parties.[3] For instance, Facebook collected phone numbers from users and publicly stated the purpose was for two-factor authentication, but the phone numbers were improperly used for advertising.[4]

[2] Data security is the protection of PI from unauthorized access or use, and the response to the unauthorized access or use of PI.[5] In 2019 alone, there were over 5,100 publicly disclosed data breaches for a total of 7.9

[1] STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019).

[2] *See, e.g.*, CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10338, FACEBOOK'S $5 BILLION PRIVACY SETTLEMENT WITH THE FEDERAL TRADE COMMISSION 2–3 (2019) (outlining the allegations set forth in the FTC's 2012 Order and 2019 Order against Facebook).

[3] Complaint for Civil Penalties, Injunction, and Other Relief, at ¶ 6, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. 2020); United States v. Facebook, Inc., 2020 U.S. Dist. LEXIS 72162, at *10 (D.D.C. 2020).

[4] Complaint for Civil Penalties, Injunction, and Other Relief, *supra* note 3, at ¶ 13.

[5] STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019).

billion exposed records, which was an increase of 33% over 2018.[6] One of the largest data breaches in recent memory—by number of individuals who had their PI stolen—was Equifax, which affected more than 147 million consumers.[7] Equifax failed to implement basic security measures and install security patches in various databases; this caused the data breach, and hackers stole names, dates of birth, social security numbers, physical addresses, telephone numbers, email addresses, and payment card data.[8] Equifax ultimately agreed to pay at least $575 million, and possibly up to $700 million, among other stipulations, in a settlement with the FTC, the Consumer Financial Protection Bureau (CFPB), and state governments.[9]

[3] Despite data privacy and security failures in recent years, Congress has not passed comprehensive legislation to protect consumers' PI. Companies collect, use, and sell PI for various purposes, which has made PI the currency of the internet.[10] However, the concept of individual privacy is not new—Samuel D. Warren and Louis D. Brandeis advocated for an

[6] Rae Hodge, *2019 Data Breach Hall of Shame: These Were the Biggest Data Breaches of the Year*, CNET (Dec. 27, 2019, 4:00 AM), https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/ [https://perma.cc/3TEC-J6YW].

[7] Equifax, Inc., Annual Report (Form 10-K) 3 (Mar. 1, 2018); *Equifax Data Breach*, EPIC.ORG (2020), https://epic.org/privacy/data-breach/equifax/ [https://perma.cc/VQ99-AYE9] (citing 148 million people affected by the breach rather than 147 million).

[8] Complaint for Permanent Injunction and Other Relief at ¶¶ 13, 21, FTC v. Equifax, Inc., No. 1:19-mi-99999-UNA (N.D. Ga. Jul. 22, 2019).

[9] Press Release, FTC, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (Jul. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/SND5-KAGY].

[10] *See* Lee Rainie & Janna Anderson, *The Fate of Online Trust in the Next Decade*, PEW RSCH. CTR. 27 (Aug. 10, 2017), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/08/PI_2017.08.10_online TrustNextDecade_FINAL.pdf [https://perma.cc/TX4B-X8MD].

individual's right to privacy in 1890.[11] Warren and Brandeis recognized the necessity "to define anew the exact nature and extent of [privacy] protection" when inventions, innovations, and business models call for advancements in privacy rights to protect the individual, because such inventions and innovations "subject [an individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury."[12] Put differently, as technology develops, privacy protections must evolve.[13]

[4] In the absence of comprehensive federal data privacy and security legislation, states are moving at an increasing rate to enact such protections.[14] Illinois enacted the Biometric Information Privacy Act (BIPA), which regulates the privacy of biometric data.[15] California enacted the California Consumer Privacy Act (CCPA), which took effect on January 1, 2020.[16] Generally, these state laws regulate the collection, use, retention,

[11] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890) ("[T]he individual shall have full protection in person and in property is a principle as old as the common law . . . .").

[12] *Id.* at 193, 195–96.

[13] *See, e.g.*, Katherine Bindley, *Your Health Data Isn't as Safe as You Think*, WALL. ST. J.: TECH (Nov. 22, 2019, 1:15 PM), https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606?shareToken=st5dafc634c9974cb1b760ed8311261a7c [https://perma.cc/K72M-SX3P] (exploring how technology is developing faster than regulators can amend legislation, for example HIPPA).

[14] *See* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 2–3, 8–9, 12 (2019) (noting how federal statutes regulating privacy protection are siloed and highlighting California's and Illinois' privacy laws).

[15] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5(g) (2008).

[16] California Consumer Protection Act, CAL. CIV. CODE ANN. §§ 1798.100–1798.199 (West 2020) (targeting companies that collect and/or sell PI and designed to protect consumers and their right to data privacy).

and dissemination of PI.[17] As of April 16, 2020, three states have enacted some form of data privacy protections for individuals, and twenty-three states were either considering data privacy legislation or formed task forces and advisory committees regarding the subject matter.[18]

[5] The enforcement of such legal protections is a hotly contested issue in data privacy and security legislation and regulation. In some cases, states empower individuals to enforce the data protections via a statutory private right of action (PROA).[19] A PROA is "[a]n individual's right to sue in a personal capacity to enforce a legal claim."[20] At the federal level, Congress permits a PROA in several of the sector-specific data privacy and security statutes (but not others such as HIPAA),[21] and Congress has proposed a

[17] *See, e.g.*, STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 38–40 (2019) (explaining the scope and requirements of California's Consumer Privacy Act).

[18] *State Comprehensive-Privacy Law Comparison: Bills Introduced 2018-2020*, IAPP (July 6, 2020), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law.pdf [https://perma.cc/77AD-KSL4].

[19] *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/20 (2008) ("Any person aggrieved by a violation of [BIPA] shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."); CAL. CIV. CODE ANN. § 1709.150, *amended by* 2019 Cal. Legis. Serv. Ch. 757 (A.B. 1355) (West 2020) ("Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of [its] duty to implement and maintain reasonable security procedures and practices . . . .").

[20] *Private Right of Action*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[21] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681n(a) (providing "[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any [individual] is liable to that [individual]" for "actual damages" or statutory damages); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (discussing the individual's right to "fair and accurate credit reporting," the obligations imposed onto credit reporting agencies to "follow reasonable procedures to assure maximum possible accuracy," and the civil liability for willful noncompliance). *See generally* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN

PROA in at least one of the omnibus federal privacy bills that has been introduced this Congressional session.[22] The question of whether to include a PROA or not has become one of the most controversial and important questions in enacting data privacy laws at the federal and state levels.

[6] Data privacy and security protections, and the enforcement of those protections, increases in importance every day. The COVID-19 pandemic provides an illustration of the increasing importance; in response to the pandemic, Apple and Google partnered together to develop and release a tracing application for iOS and Android devices.[23] Governments around the world sought and implemented contact tracing systems that collect, store, and use geolocation and health data.[24] The collection, storage, and usage of PI increases as the world develops and demands new technologies, such as contact tracing applications in response to a pandemic, which in turn, increases the importance of keeping that PI safe, private, and secure.

[7] This paper discusses the PROA with respect to data privacy and security legislation, without regard to whether such legislation is enacted at a state or federal level. This paper does not discuss the arguments for or against the need for data privacy and security legislation. Rather, the need for such protections is assumed by the premise that a federal or state legislature plans to adopt protective legislation, and thus has already made the decision that such protections are necessary.

INTRODUCTION at app. (2019) (providing a comprehensive list of sector-specific data protection laws and noting that other sector-specific data privacy and security statutes, such as HIPPA, do not include a PROA).

[22] *See, e.g.*, S. 1214, 116th Cong. § 17 (2019) (referred to the S. Comm. on Com., Sci., and Transp. on April 11, 2019, but the committee has not advanced the bill).

[23] Ben Kochman, *Apple, Google Launch COVID-19 Exposure Notification Tool*, LAW360 (May 20, 2020, 10:29 PM), https://www.law360.com/articles/1275597/apple-google-launch-covid-19-exposure-notification-tool [https://perma.cc/26GK-MKAM].

[24] *See id.*

[8] The purpose of this paper is to discuss that if a legislature decided to enact privacy legislation, what enforcement mechanisms can make that legislation most effective. Throughout this article, I revisit the Facebook and Equifax cases to illustrate the arguments presented herein. Part I discusses three benefits and three drawbacks to including a PROA in data privacy and security legislation. Part I is not an exhaustive or in-depth discussion regarding the benefits and drawbacks. Part I concludes that PROA, with limitations, balances individual protections against the judicial economy and burdensome litigation against businesses. Having concluded that a limited PROA is necessary, Part II explores two issues with implementing a limited PROA—standing and monetary remedies. Part II concludes by determining the injury-in-fact requirement for standing does not inhibit a PROA, and monetary remedies should be prescribed to effectuate the protections.

II. WHY ENACT A PRIVATE RIGHT OF ACTION

[9] Data privacy and security legislation should include a PROA because it is a scalable and effective enforcement mechanism that would help to better protect the privacy and security of individuals' PI. Three benefits of a PROA are discussed herein. First, a PROA will serve a deterrent function and will incentivize organizations to implement best-in-class data privacy and security practices and capabilities to avoid litigation. Second, a PROA will serve as an additional enforcement mechanism, which in turn, will drive industry compliance with any federal or state legislation. Third, a PROA will improve public trust in businesses through transparency and accountability.

[10] However, a PROA has drawbacks—three of which are discussed herein. First, a PROA would increase litigation. Second, it may lead to some unjustifiable litigation. Third, a PROA may cause undesirable social effects. Therefore, when weighing the benefits and drawbacks against each other, a PROA would be beneficial overall. However, a PROA must be carefully crafted and have limitations to mitigate against the drawbacks.

A. Benefits of a Private Right of Action

[11] A PROA will serve a deterrent function. Businesses will look to avoid potential litigation and liability by proactively implementing reasonable privacy and security practices and capabilities. For the purposes of this discussion, "practices and capabilities" is defined broadly and includes privacy and security disclosures, policies, procedures, functions, processes, and abilities. In general, business models focus on profit-making and governments focus primarily on national security (federal government only) and economic prosperity (both federal and state governments); this leaves little attention to individual rights, such as data privacy.[25] ~~The~~ Lack of attention has led to the current data privacy and security regime in the United States, which consists of a "patchwork" of federal laws—regulating specific industries and categories of PI—mixed with limited state laws.[26] Under the present U.S. regime, the individual maintains weak bargaining power and almost no leverage because the individual has little control over the use and dissemination of his or her data, yet the individual bears the risks of poor privacy and security practices if the data is improperly used or accessed.[27]

[12] From an economic perspective, the possibility of litigation can deter certain behaviors when the costs of those behaviors outweigh the benefits.[28] Under the present regime, businesses reap great profits (benefits) from the use, sale, or dissemination of PI and do not face substantial loss (costs) from

[25] *See* Rainie & Anderson, *supra* note 10, at 16-17.

[26] *See* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019).

[27] Rainie & Anderson, *supra* note 10, at 17 (quoting Henning Schulzrinne, professor at Columbia University).

[28] *See generally* Thomas C. Galligan, Jr., *Deterrence: The Legitimate Function of the Public Tort*, 58 WASH. & LEE L. REV. 1019, 1032 (2001) (discussing the deterrence function of public tort law).

poor data privacy and security practices because the individual, not the business itself, bears the risk.[29] A PROA would disrupt this cost-benefit analysis and tilt decisions towards greater protection of data privacy and security—otherwise, businesses would face the potential of greater costs resulting from litigation.[30] Businesses would be incentivized to prevent such costs by investing in improved data privacy and security practices and capabilities.[31]

[13] Further, litigation develops the law.[32] Litigation creates and advances a common set of industry principles, which in turn improves industry practices and capabilities.[33] The medical industry's adoption of X-ray technology demonstrates this concept.[34] Before the profession's discovery and adoption of X-ray technology, internal injuries were difficult

[29] *See* Press Release from Rebecca Kelly Slaughter, Comm'r, FTC, Dissenting Statement: In the Matter of FTC vs. Facebook, 7–8, 12 (July 24, 2019) [hereinafter Slaughter Dissent], https://www.ftc.gov/system/files/documents /public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf [https://perma.cc/5XXN-W4DB] (discussing that while Facebook's $5 billion penalty from a settlement with the FTC was larger than any other penalty in Commission history, it was insignificant when compared against Facebook's monthly earnings).

[30] *See e.g.*, Nick Statt, *Facebook Sets Aside $3 Billion Ahead of Record FTC Fine Over Privacy Violations*, THE VERGE (Apr. 24, 2019, 4:24 PM), https://www.theverge.com/2019/4/24/18514805/facebook-q1-2019-earnings-ftc-record-fineprivacy-violations-3-billion [https://perma.cc/9AKD-28QF] (showing that upon the FTC's announcement of the settlement and $5 billion fine with Facebook, Facebook's stock increased, reaping the type of benefit that a PROA would jeopardize).

[31] *See* Galligan, Jr., *supra* note 28.

[32] *See* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 981–83 (2016).

[33] *See id.*

[34] *See id.* at 1009.

to detect and diagnose.[35] X-ray technology changed medicine by showing medical professionals internal injuries, and courts were quick to incorporate the new technology into the doctors' duty of care.[36] Within a few years, any doctor who failed to use the technology in the diagnosis would face liability if the failure harmed the patient.[37] Here, litigation resulted in a new requirement for the entire industry.[38] The industry had to invest in adopting the new requirement. Likewise, data privacy and security litigation would advance industry requirements with the goal of preventing future harms onto individuals. A PROA would deter poor practices and capabilities while incentivizing investment in best-in-class privacy and security capabilities and raising the industry's duty of care by developing and advancing the law.[39]

[14] But some scholars argue that litigation will not develop the law as intended because privacy and security practices and capabilities will still become, as they exist today, symbolic structures of compliance rather than substantive protections that actually protect PI.[40] In other words, privacy and security practices and capabilities have morphed into a managerial process of completing compliance checklists, internal audits, and industry questionnaires.[41] Rather than incentivizing investment into best-in-class

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *See id.* at 1010.

[39] *See generally* Galligan, Jr., *supra* note 28, at 1032 (analyzing the application of deterrence in economic theory to tort law).

[40] *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. UNIV. L. REV. 773, 776 (2020).

[41] *See id.* at 776–77 ("[C]ompanies create structures, policies, and protocols that comply with the law in name only . . . [and] provide little to no protection.").

privacy and security capabilities, a PROA would incentivize companies to further develop more symbolic structures versus actual technological protections for individuals. Furthermore, as technology companies argue that their symbolically structured compliance practices and capabilities make them compliant with the substantive law, lawyers and judges become more likely to defer to these toothless symbolic structures created by the corporations themselves that do not actually protect individuals.[42]

[15] While litigation may result in more symbolic structures of compliance, the same scholars recognize that a PROA is necessary and beneficial to advancing substantive protections for consumers.[43] This is because a PROA must be a part of overall legal reform with respect to privacy and security protections—it cannot stand alone.[44] Similar to X-ray technology in medicine or products liability claims in the pharmaceutical industry, liability-based incentives, like litigation, encourage efficient and compliant behavior.[45]

[16] If the foregoing cost-benefit analysis fails to incentivize businesses to *proactively* invest in improved data privacy and security, a PROA would

[42] *Id.* at 778.

[43] *See, e.g.*, *id.* at 831 ("Therefore, any new privacy law must include a private right of action [because] . . . giving individuals the opportunity to realize their rights in court has worked in the past.").

[44] *See id.* at 826–34 (listing several methods to solve the symbolic structure problem: reforming the substantive law, permitting rulemaking for the FTC, reforming the FTC, empowering individuals with a PROA, and instilling privacy and security as part of the ethos of a company).

[45] *See* Steven Garber, *Economic Effects of Product Liability and Other Litigation Involving the Safety and Effectiveness of Pharmaceuticals*, RAND INST. FOR CIV. JUST., 79 –80 (2013).

provide an additional *reactive* enforcement mechanism.[46] This reactive enforcement mechanism would drive compliance with data privacy and security legislation. The present regime needs an additional enforcement mechanism because (i) the FTC's enforcement is limited, (ii) there is a lack of precedential force of law to drive industry compliance, and (iii) the industry's self-regulation approach has failed.

[17] First, the FTC, as the de facto privacy enforcement agency of the federal government, [47] is limited in two major ways. First, under the Federal Trade Commission Act (FTC Act), its enforcement authority extends only to "unfair or deceptive[business] acts or practices."[48] In the FTC's enforcement, the FTC can enforce actions against companies using the "unfairness prone" provided in the FTC Act. However, under the "deceptive prone" of the FTC Act, the FTC is often powerless unless a company discloses its privacy practices and then fails to follow them.[49] Second, the FTC is resource constrained; only 40 full-time FTC employees are dedicated to internet privacy and data security.[50] Its limited resources force the FTC to target businesses that are substantially harming consumers and

[46] *See generally* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L. J. 653, 683–85 (2019) (discussing the effect of remedies on privacy rights, especially with the FTC's limited ability to hear cases).

[47] FTC, PRIVACY & DATA SECURITY UPDATE: 2018 2 (2018) [hereinafter FTC UPDATE], https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/9GNT-YM9V].

[48] *Id.*; 15 U.S.C. § 45(a)(1-2) (2019).

[49] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2114 (2003); HURWITZ, *supra* note 32, at 963–66 (discussing an overview of the FTC's unfairness authority).

[50] Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, THE HILL (Apr. 3, 2019, 11:01 AM), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security [https://perma.cc/66YW-KGCN].

cases that have a high likelihood of success.[51] Therefore, many companies and deceptive business practices go uninvestigated.

[18] The "unfair and deceptive" statutory limitation and the resource constraint curtail the FTC's enforcement in driving legal compliance; consequently, there is a gap in the FTC's enforcement authority. A PROA would fill this gap by allowing individuals to enforce their protections.

[19] Second, a PROA would drive compliance because a PROA would result in court opinions that carry greater precedential force than administrative agency actions. For example, administrative agencies may rely on rule-making authority or adjudications to advance policy positions, interpretations, and decisions. However, the FTC does not have the "conventional" rule-making authority. Rather, the FTC is limited by the burdensome Magnuson-Miss rule-making procedures, which are so procedurally burdensome that the FTC has not engaged in rule-making for decades.[52] Instead, the FTC relies on consent decrees that often include vague requirements.[53] But generally, an administrative agency can deviate from its past policy positions, interpretations, and decisions, or with respect to the FTC, its prior positions in consent decrees. But such deviations are subject to the arbitrary and capricious standard if challenged in judicial review.[54] Per *Chevron*, the court must defer to the agency if the agency's reasoning is not unreasonable and Congress has not spoken on the issue.[55]

---

[51] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 609, 613 (2014).

[52] Waldman, *supra* note 40, at 828.

[53] *Id.* at 796.

[54] *See* Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc., 468 U.S. 837, 843–44 (1984).

[55] *See id.* at 842–44. (establishing the "Chevron Deference" test as to when a court must defer to an agency's action if such action is not arbitrary or capricious so long as Congress has not spoken on the matter).

In other words, an agency has more flexibility to change course so long as its reasoning behind the change is reasonable.

[20] However, the judiciary maintains a higher standard to change course with respect to prior court opinions per *stare decisis*. To overturn settled doctrine, a court bound to that precedent must have significant justification.[56] Therefore, court opinions carry a greater precedential force than administrative agency actions because an agency can change course so long as its reasoning is reasonable, but a court cannot change prior court opinions unless it has significant justification.

[21] Moreover, the FTC's enforcement actions often lack the precedential force for other businesses because an FTC consent decree functions as a contract between the FTC and the alleged business rather than binding precedent that would apply to *every* business.[57] While some scholars argue the FTC enforcement is sufficient because it is common law-like,[58] this argument is flawed. The Third Circuit Court of Appeals noted the FTC consent decrees fail to provide "ascertainable certainty" regarding the interpretation of what specific privacy and security practices fail the FTC's expectations.[59]

[22] But as previously discussed, court opinions carry greater precedential force. Opinions create true common law that converges around

[56] Citizens United v. FEC, 558 U.S. 310, 408 (2010) (Stevens, J., dissenting) ("[I]f [*stare decisis*] is to do any meaningful work in supporting the rule of law, it must at least demand a significant justification . . . for overturning settled doctrine.").

[57] *See* Solove & Hartzog, *supra* note 51, at 607.

[58] *See id*. at 619 (discussing how the FTC's memorialized outcomes are the functional equivalent to common law).

[59] Hurwitz, *supra* note 32, at 976 (the FTC's consent orders "were of little use to [defendants] in trying to understand the specific requirements imposed by [section 5 of the FTC Act]." (quoting Wyndham Worldwide Corp., 799 F.3d at 252-53, 255 (3rd Cir. 2015))).

a common set of industry principles over time.[60] Here, common law would create stable precedent that would provide fair notice to the businesses that are bound to it.[61] Even though businesses have called for the FTC to be the sole enforcer of data privacy and security laws,[62] this would not successfully effectuate such legal protections because the FTC's enforcement is limited and there would be no true common law.

[23] Third, while businesses self-regulate data privacy and security practices through trade associations and certification programs, the number of high-profile data privacy lapses and data breaches indicate a private market failure with respect to the compliance and enforcement. This may be because industry association guideline and certification programs have almost no effect on improving a business's privacy and security practices.[63] While the industry guideline and certification programs may improve a business's trustworthiness in the eyes of the consumer, this trust is blind and misplaced.[64] Privacy trade groups frame compliance with privacy and security laws as a means of reducing corporate risk—not a means of actually protecting individuals' PI by improving a business's privacy and security

[60] *See id*. at 980 (asserting that the FTC's approach to creating a common set of principles through its case-by-case adjudication is similar to how an actual court would create common law).

[61] *See id*. (stating that common law, or an even more concrete Supreme Court ruling, would aid in guiding businesses by creating a stable precedent).

[62] *See Framework for Consumer Privacy Legislation*, BUS. ROUNDTABLE 4, https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf [https://perma.cc/B6E9-EQDH].

[63] *See* Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 15, 25-26 (2015) (discussing an empirical study of whether certification programs and trade associations improve data privacy and security performance).

[64] *See generally* Waldman, *supra* note 40, at 800 (demonstrating a "check-the-box" type approach to privacy law compliance).

practices.[65] The fundamental issue with self-regulation is the conflict of interest that exists—the regulators are the regulated. Here, actually protecting individuals' PI by improving a business's privacy and security practices (e.g., prohibiting the processing and dissemination of PI in certain situations) is at conflict with the regulators' (the businesses themselves via trade associations) source of revenue. It is counterintuitive for businesses to improve their privacy and security practices and capabilities if such improvements negatively impact their revenue and profits.

[24] While proponents of self-regulation will argue that the conflict of interest can be avoided by including stakeholders with different interests or business models, this is not applicable with privacy and security protections.[66] This is because the collection, use, and dissemination of PI is at the core of businesses' profit motives. For example, Facebook may have a different business model than Equifax, but the revenue and monetization models for both companies rely on the collection and use of PI on their platforms and with their products. The same proponents recognize that self-regulation is unlikely to satisfy the proponents of government regulation intended to protect *fundamental human rights*, like privacy and security.[67] Therefore, the private market failure with respect to self-regulation exists because this conflict of interest prevents the businesses from actually protecting individuals versus themselves.

[25] To rectify a private market failure, when the market is unable or unwilling to deliver the necessary technological innovation or other remedies to improve the status quo, sometimes government intervention is

[65] *Id.*

[66] *See* Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising*, THE INFO. TECH. & INNOVATION FOUND. 7 (Dec., 2011), https://itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf [https://perma.cc/Y6R4-H2XF].

[67] *See id.* at 8.

necessary.[68] However, government *mandates* via legislation and regulation (as distinguished from government *intervention*) that prescribe the adoption of certain technologies, practices, or capabilities can be counterproductive.[69]

[26] With the FTC's enforcement limitations and the self-regulation market failure, a PROA would add an additional enforcement mechanism—private causes of action and the judiciary—to uphold individuals' privacy and security rights. Here, the substantive law would create the duty to protect such rights, and a PROA provision in the substantive law would be a form of government *intervention*, but not a government *mandate*, because the government would be intervening by permitting another type of enforcement mechanism, but not prescribe the technologies that the market must adopt.[70]

[27] Furthermore, litigation would provide a public benefit in two ways: (i) it would improve public trust; and (ii) as previously discussed, the improved privacy and security industry standards would reduce public harm.

[28] First, a PROA would improve public trust in businesses by increasing transparency and introducing public accountability.[71] Only 24% of Americans believe that technology firms, in particular, sufficiently

[68] *See generally* Gary E. Marchant, *Complexity and Anticipatory Socio-Behavioral Assessment of Government Attempts to Induce Clean Technologies*, 61 UCLA L. REV. 1858, 1860–62 (2014) (arguing that government mandates should be a last resort to stimulate technology innovation).

[69] *See id.* at 1892 ("Government attempts to [mandate technological innovation] are . . . hazardous undertakings," because such attempts are often "plagued by opposition, delays, unanticipated impacts, and controversies.").

[70] *See generally* Marchant, *supra* note 68, at 1892 (demonstrating the risk and challenges of government mandates pertaining to rapidly changing technologies).

[71] *See* Slaughter Dissent, *supra* note 29, at 3.

protect PI, and only 3% trust technology firms to do the right thing just about always.[72] Public distrust in businesses—specifically in technology firms—likely stems from two sources: (a) past violations of individuals' data privacy expectations,[73] and (b) a lack of information about the business' actual privacy practices.[74]

[29] While the FTC's enforcement actions, like the Facebook settlement, make *some* information public through allegations, complaints, and consent decrees, the actions are insufficient in putting *enough* information into the public domain for the public to understand how data is truly collected, used, sold, and protected (or not)—the public is still largely left in the dark.[75] For example, Facebook's 2019 settlement with the FTC did not require Facebook to publicly disclose: (a) the specific PI collected, (b) the method and purpose for collecting PI, (c) the use of the PI, (d) how long Facebook stores PI, and (e) how individuals can access or delete their PI.[76] While substantive privacy laws can mandate the disclosure of such information, the disclosure of specific policies and practices (e.g., how the PI is handled, who specifically has access to the PI, and where the PI is stored) is likely to be excluded from the mandatory disclosures under any substantive privacy laws. When the public is informed about these specific policies and

[72] *See* Aaron Smith, *Public Attitudes Toward Technology Companies*, INTERNET & TECH. (June 28, 2018), https://www.pewresearch.org/internet/2018/06/28/public-attitudes-toward-technology-companies [https://perma.cc/TYX2-SL5Q] (discussing the lack of trust in technology platforms).

[73] *See* Fed. Trade Comm'n, Dissenting Statement of Comm'r Rohit Chopra, In re Facebook, Inc. Commission File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [https://perma.cc/AY35-EPCT].

[74] *See* Slaughter Dissent, *supra* note 29, at 13–14.

[75] *See generally id.*, at 8–12 (demonstrating the deterrence factors of the Facebook settlement).

[76] *Id.* at 13.

practices, only then can the public understand the violations of privacy rights sufficiently to enforce the individuals' rights and pressure policymakers to enact further data privacy and security legislation.[77]

[30] These specific policies and practices—in addition to other valuable information—would enter the public domain through discovery of important documents, testimony, and relevant evidence.[78] For example, product-liability litigation in the pharmaceuticals industry has uncovered mountains of evidence of questionable practices by drug manufacturers.[79] These questionable practices included withholding or distorting drug safety information, the results of clinical trials, and the frequency and severity of side effects.[80] Another example is the tort litigation against DuPont de Nemours (commonly known as "DuPont") for their Teflon products.[81] Discovery uncovered DuPont knew the dangers of PFOA or C8, which is the chemical used in Teflon, after conducting its own research studies.[82] Through discovery and the actions of the litigation's persistent lawyer, Rob Bilott, the public learned of DuPont's actions that posed an imminent and substantial threat to public health and the environment.[83]

---

[77] *See generally* Statement of Chairman Joe Simons and Comm'rs Noah Joshua Phillips and Christine S. Wilson, Fed. Trade Comm'n 6 (July 24, 2019) (discussing how Congress should evaluate the collection, use, aggregation, and monetization of PI).

[78] *See* Slaughter Dissent, *supra* note 29, at 7.

[79] *See* Garber, *supra* note 45, at 60.

[80] *See id.* at 80.

[81] *See* Nathaniel Rich, *The Lawyer Who Became DuPont's Worst Nightmare*, N.Y. TIMES (Jan. 6, 2016), https://www.nytimes.com/2016/01/10/magazine/the-lawyer-who-became-duponts-worst-nightmare.html [https://perma.cc/4XPT-F6ZL].

[82] *Id.*

[83] *Id.*

[31] While some cases will settle before discovery, for the cases that proceed to discovery and trial, *more* information regarding a business's practices, policies, and capabilities would enter the public domain than otherwise would have had it not been for a PROA.[84] While publicizing a business's practices, policies, and capabilities may inform hackers of a business's vulnerabilities, such information would likely only enter the public domain after a breach occurred and presumably after the vulnerability was remedied. The potential liability and broad public dissemination of any poor privacy and security practices, policies, and capabilities, would further deter businesses from future violations.[85]

[32] Second, as previously discussed, the development of precedents would lead to the advancement of industry standards. Businesses would be required to adopt the new industry standards—shaped and created by judicial decisions, not legislatively or quasi-legislatively.[86] Changing industry standards legislatively or quasi-legislatively would be a nearly impossible task for a legislature or administrative agency because it would require constant assessment of new technologies..[87] Litigation, on the other hand, provides a positive public externality—a social benefit beyond that

[84] *See* Lee Levine et al., *Newsgathering and the Law*, § 6.01(2), 5th ed. MATTHEW BENDER & COMPANY (2018) (while proprietary information would be protected from public disclosure, a PROA would still put *more information* into the public domain. Court records are "presumed to be open to the general public.").

[85] *See generally* Slaughter Dissent, *supra* note 29, at 7; Tom Popmaronis, *Billionaire Warren Buffett has a 'Simple' Test for Making Tough Decisions—Here's How it Works*, CNBC (May 11, 2019), https://www.cnbc.com/2019/05/10/billionaire-warren-buffett-use-this-simple-test-when-making-tough-decisions.html [https://perma.cc/N58D-D4BG] (publicizing poor data privacy and security practices poses an intangible risk to the business's brand and reputation. Here, businesses would be deterred from poor practices because no business wants to end up on the front page of a newspaper).

[86] *See generally* Hurwitz, *supra* note 32, at 982.

[87] *See id.* at 1010–11.

which is reflected in the litigants' private gains.[88] Litigation focuses on the gray areas of law—where disputes arise—and courts decide cases, upholding, establishing, or advancing industry standards, because they must.[89] Litigation would present a constant stream of cases where litigants have an incentive to see cases through decision.[90] Legislatures and the FTC do not share this. The public is not necessarily getting the best protection under the present regime because the FTC only pursues a limited set of high-priority cases and legislatures focus on other priorities.[91]

[33] Therefore, for the foregoing reasons, a PROA would effectuate the data privacy and security protections by deterring poor practices and capabilities, serving as an additional enforcement mechanism, and helping to develop and advance industry standards.

B. Drawbacks of a Private Right of Action

[34] While the PROA would provide the foregoing benefits, a PROA would have drawbacks. The drawbacks discussed herein are: a PROA would (i) *increase* litigation; (ii) lead to some *unjustifiable* litigation; and (iii) result in socially undesirable effects. These drawbacks can be mitigated by carefully crafting and limiting the PROA.

[35] First, a PROA would increase litigation and burden an already slow and backlogged judiciary. To illustrate this drawback, I turn to BIPA. In January 2019, the Illinois Supreme Court held in *Rosenbach v. Six Flags Entertainment Corporation*, that a plaintiff need not allege any actual injury or adverse effect beyond the statutory violation of his or her privacy right

[88] *See id.* at 982.

[89] *See id.* at 984.

[90] *See* Hurwitz, *supra* note 32, at 986.

[91] *See supra* Part I.A.

under BIPA.[92] *Rosenbach* was an inflection point; before *Rosenbach* (from 2008 until January 2019), there were 173 BIPA class action filings over this 11 year period, and after *Rosenbach* (January 2019 to present), there were 151 BIPA class action filings in less than one year.[93] BIPA's dramatic increase in class action filings after *Rosenbach* shows that when the door is opened for plaintiffs to sue, there is a substantial increase in litigation.

[36] Prior to *Rosenbach*, Illinois introduced an amendment to BIPA (SB 3053) to reduce the litigation and help some businesses avoid liability. While SB 3053 failed, it would have exempted businesses from liability if the business used the biometric data for certain purposes, did not profit from the biometric data, or stored the biometric data in the same or more protective manner than the business did other confidential and sensitive information.[94] This type of limitation may be helpful to avoid a tidal wave of litigation with a PROA.

[37] While a PROA would increase litigation, the litigation would have longer-term benefits, such as the development of the law, as previously discussed.[95] Eventually the law becomes sufficiently developed to produce settlements between private litigants, and when such settlements are possible, there is little incentive for parties to invest in formal litigation.[96]

---

[92] Rosenbach v. Six Flags Ent. Corp., 129 N.E. 3d 1197, 1207 (Ill. 2019).

[93] Gerald L. Maatman, Jr. et al., *Biometric Privacy Class Actions by The Numbers: Analyzing Illinois' Hottest Class Action Trend*, SEYFARTH SHAW LLP: WORKPLACE CLASS ACTION BLOG (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/ [https://perma.cc/P3AM-YXM3].

[94] S.B. 3053, 100th Gen. Assemb., Reg. Sess. (Ill. 2018) (including if the biometric data is "used exclusively for employment, human resources, fraud prevention, or security purposes.").

[95] *See supra* Part I.A.

[96] *See* Hurwitz, *supra* note 32, at 983–84.

While settlements may negate the public benefit of promoting trust and accountability, this only occurs *after* the body of law has sufficiently developed and businesses are bound by the precedential force of law, which in itself is a benefit of a PROA.[97] However, more settlements would lessen the judiciary's burden.

[38] To mitigate the increase in litigation, a PROA could be limited by a short statute of limitations,[98] narrowly defining the sufficient conditions to file a claim (like Illinois considered with SB 3053), or prescribing a process in which a plaintiff must follow before proceeding with a claim (e.g., seeking redress through an administrative agency or requiring a preliminary showing).

[39] Second, a PROA would create unjustifiable liability for businesses because individuals do not care about the exposure of their PI (e.g., if the individual affirmatively consents) or do not manifest behaviors that demonstrate the individuals are truly concerned about their privacy ("the privacy paradox").[99] In other words, why should a business be held liable when the individuals do not care about their own PI? Some scholars assert individuals fall into two categories when asked about their privacy protections: (1) individuals who are lying to themselves about their concerns over PI privacy when their behaviors demonstrate that they prefer

[97] *See supra* Part I.A.

[98] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 757 (2018) (understanding that a shorter statute of limitations may be counterproductive because the harm may occur beyond the statute of limitations).

[99] *See* John Naughton, *The Privacy Paradox: Why Do People Keep Using Tech Firms That Abuse Their Data?*, THE GUARDIAN (May 5, 2019, 2:00), https://www.theguardian.com/commentisfree/2019/may/05/privacy-paradox-why-do-people-keep-using-tech-firms-data-facebook-scandal [https://perma.cc/PP6N-MQBY]; *see also* Ignacio Cofone & Adriana Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1493 (2018) (arguing the privacy paradox results from consumers' non-belief in the law of large numbers).

the status quo and do not care about the exposure of their PI; or (2) individuals who truly care about the exposure of their PI, but participate anyways in the status quo because it is not worth their time, expense, and social cost not to engage in the modern world.[100]

[40] For instance, despite Facebook's privacy fumbles,[101] Facebook's daily active users increased after Facebook was scrutinized and prosecuted for its deceptive privacy practices, meaning users continued to share PI with Facebook.[102] This privacy paradox—"the relationship between individuals' intentions to disclose [PI] and their actual [PI] disclosure behaviors"—prompts the question as to whether a PROA would create unjustifiable liability exposure for businesses.[103] If individuals behave in a manner that demonstrates no care for their data privacy and security, then why should a legislature grant individuals a PROA?

[41] Even with the privacy paradox and the possibility of a PROA leading to some unjustifiable litigation, the foregoing benefits to the PROA are not negated.[104] The potential limitations on a PROA discussed above

[100] Scholz, *supra* note 46, at 683.

[101] *See supra* Introduction ¶ 1

[102] *See* Facebook, Inc., Annual Report (Form 10-K) (Jan. 31, 2019) (global daily active users increased 9% year-over-year).

[103] *The privacy paradox and how you can use it to increase conversion*, KEEP IT USABLE: LEARN UX (n.d.), https://www.keepitusable.com/blog/privacy-paradox-and-how-you-can-use-it-to-increase-conversion/#:~:text=The%20privacy%20paradox%20is%20the,disclosure%20behaviours%2C%20which%20are%20often [https://perma.cc/GVC9-U2FM]; *see* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1039 (2017).

[104] *See supra* Part I.A.

could also apply here in minimizing unnecessary litigation under the privacy paradox.

[42] Third, a PROA may lead to socially undesirable effects, such as higher prices for consumers. For example, typically product liability claims lead to the increase in product prices as a result of the litigation costs and damages because the liable business likely attaches the new costs from the litigation to the product itself.[105] In the extreme, the price increases could be so high that they would discourage consumers from purchasing the product.[106] However, with respect to protecting consumers' privacy and security, PI is often *how* businesses generate revenue. In other words, the product is the PI.

[43] Returning to Facebook, Facebook monetizes its users' PI by allowing advertisers to target very specific audiences. Here, the consumer does not pay the monetary price—the advertiser pays the monetary price. In more traditional product liability claims, the consumer pays the monetary price in exchange for the product when the consumer purchases the product. However, with PI, other businesses (e.g., Facebook's customers), not consumers, would pay the increase in the product's price because the advertisers are *how* companies generates revenue using PI.

[44] Some of the other businesses may not have the appetite to pay the increase in prices that result from a PROA. For instance, Facebook may lose some of its customers (e.g., advertisers) because the cost of ads increased. Equifax may lose some of its customers (e.g., businesses that purchase credit bureau data on consumers) because the cost of maintaining the PI increased. However, this is the socially *desirable* effect. If the demand for PI, and the products that leverage the PI, decrease, then the decrease in the

[105] *See* A. Mitchell Polinsky & Steven M. Shavell, *The Uneasy Case for Product Liability*, 123 HARV. L. REV. 1436, 1459–1460 (2010).

[106] *See id.* at 1471–1472 (leading the manufacturer of the product to potentially withdraw the product from the market or go out of business because continuing would no longer be profitable).

demand for PI would result in a decrease in the risk for the consumer. In addition, if a PROA increases product prices for businesses that collect, use, and disseminate PI, then those businesses would be incentivized to avoid litigation; this is the goal of a limited PROA in the first place.

[45] Therefore, considering the foregoing drawbacks, a limited PROA is necessary because it effectively balances the benefits of a PROA against the drawbacks. The limitations could include a shorter statute of limitations, narrowly defining the conditions to file a claim, and prescribing a process in which a plaintiff must follow prior to filing a claim.

III. IMPLEMENTATION ISSUES WITH A PRIVATE RIGHT OF ACTION

[46] Having established a limited PROA is necessary in data privacy and security legislation, I turn next to two implementation issues with a PROA: standing and monetary remedies. To establish standing, the injury must be concrete and particularized.[107] Data privacy violations are often particularized,[108] but not concrete because such violations are intangible. Moreover, if an individual's rights to data privacy and security are violated, absent a clear economic harm, a monetary remedy would be difficult to calculate. Part II.A discusses how a plaintiff can establish the injury-in-fact requirement for standing. Part II.B discusses why monetary remedies are necessary to effectuate data privacy and security protections, and why damages versus other monetary remedies should be expressly prescribed in law.

[107] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).

[108] *See id.* at 1548 ("For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" (quoting Lujan v. Def. of Wildlife, 504 U.S. 555, 560, n.1 (1992)).

A. The Injury-in-Fact Requirement for Standing

[47] Any legislation must expressly grant a plaintiff the right to sue to enforce statutory rights, but a plaintiff is still required to establish standing.[109] To establish standing in federal court, the plaintiff must show, among other things, that he or she suffered an injury-in-fact—that is an actual or imminent injury that is concrete and particularized.[110] The primary purpose of the standing doctrine is to prevent the judiciary from disturbing the separation of powers between the political branches by adjudicating abstract or hypothetical disputes.[111]

[48] The United States Supreme Court recently discussed the injury-in-fact requirement in a case related to data. In *Spokeo Inc. v. Robins*, the issue was whether a credit reporting agency's continuous data inaccuracy regarding the plaintiff's PI was concrete and particularized for the plaintiff to have standing.[112] The parties only disputed whether the plaintiff's alleged

[109] *See* Raines v. Byrd, 521 U.S. 811, 820, n.3 (1997) ("[C]ongress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.").

[110] *See Lujan*, 504 U.S. at 560–561 (stating that to establish standing the plaintiff must have (1) suffered an injury-in-fact; (2) that is fairly traceable to the defendant's conduct; and (3) that is redressable by the court); *see also de facto*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[111] *See Spokeo, Inc.*, 136 S. Ct. at 1547 (stating that Article III of the United States Constitution provides the judicial power extends only to "Cases and Controversies," and the standing doctrine is the traditional understanding of a case or controversy); Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459, 468 (listing three purposes of standing: (1) "to ensure [the] plaintiff has a sufficient stake in the controversy;" (2) "to prevent the federal courts from engaging in decisions that are better made by the political branches;" and (3) "to prevent Congress from conscripting the courts to fight its battles against the executive branch").

[112] *See Spokeo, Inc.*, 136 S. Ct. at 1544 (explaining that the plaintiff sued under the PROA provided in the FCRA and alleged the credit reporting agency's failure to correct his PI intangibly harmed his employment prospects).

injury was concrete because it was clear the alleged injury was particularized to the plaintiff.[113] The Court stated that an intangible injury can be concrete, and courts should consider the history and Congressional judgment to determine whether an intangible harm constitutes an injury-in-fact.[114] Congress can define injuries (e.g., by elevating intangible harms to injuries-in-fact) and determine chains of causation that give rise to a case or controversy where none existed before.[115] Should a legislature define a data privacy statutory violation as an intangible injury, the plaintiff need not allege any additional harms beyond the one the legislature has identified and elevated.[116] Further, the concrete-harm requirement need not be applied rigorously when a plaintiff seeks redress for an alleged violation of his or her statutory rights because the constitutional separation of powers concerns are not implicated.[117]

[49] Generally, alleging a concrete harm is difficult for plaintiffs because victims of data breaches and privacy violations often do not suffer a clear and immediate pecuniary or reputational harm.[118] Further, alleging a

[113] *See id.* at 1548 (noting the Ninth Circuit Court of Appeals only analyzed whether Robins' injury was particularized, that is affecting the plaintiff individually, inferring that the particularization element was not in dispute at the Supreme Court).

[114] *See id.* at 1549.

[115] *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring); *see, e.g.*, 17 U.S.C § 501(b) (The copyright's legal owner "is entitled to institute an action for any infringement . . . .").

[116] *Spokeo, Inc*, 136 S. Ct. at 1549; *see* Scholz, *supra* note 46, at 654 (discussing other "causes of action that do not require plaintiffs to show harm beyond the violation of their legal rights: . . . misuse of confidential information, . . . infringement of intellectual property, [and] trespass . . . .").

[117] *Spokeo, Inc*, 136 S. Ct. at 1552 (Thomas, J., concurring).

[118] *See, e.g.*, Solove & Citron, *supra* note 98, at 739 ("The concept of harm . . . from a data breach has confounded . . . courts. There [is] no consistent or coherent judicial approach to data-breach harms. More often than not, a plaintiff's increased risk of financial injury and anxiety is . . . insufficient to warrant recognition of harm . . . .").

particularized harm may be difficult for plaintiffs because victims of data breaches and privacy violations must ascertain whether their PI was included in a breach or privacy violation. To satisfy the particularized harm requirement, plaintiffs must allege that the defendant violated the plaintiff's statutory rights—not a generalized grievance.[119] The difficulty in ascertaining this may vary for would-be plaintiffs.

[50] Therefore, if policymakers provide for data privacy and security protections, to effectuate the protections under a PROA, policymakers must elevate the intangible harm to injury-in-fact status. If policymakers elevate the violation of an individual's data privacy and security rights to an injury-in-fact and would-be plaintiffs ascertain whether their own PI was affected, there should not be a constitutional limitation for plaintiffs to establish standing (assuming all other requirements for standing are sufficiently met).[120]

B. Monetary Remedies

[51] Should a plaintiff succeed on a claim, courts would face the second issue with implementing a PROA—the difficult task in calculating remedies. Remedies would be difficult to determine because a violation of an individual's data privacy and security rights would be an intangible injury.[121]

[52] But a PROA should not be without remedies, even if the intangible injury is difficult to quantify, because any privacy and security laws would be worthless if remedies were not attached to the enacting legislation.[122] If

[119] *See Robins v. Spokeo, Inc.*, 742 F.3d 409, 413 (9th Cir. 2014).

[120] *See, e.g.*, *Spokeo, Inc*., 136 S. Ct. at 1540.

[121] *See supra* Part II. A.

[122] *See* Scholz, *supra* note 46, at 657.

policymakers afford the right to data privacy and security to individuals, "[a] right is no right without a remedy."[123]

[53] When the injury is intangible and difficult to quantify, courts need guidance as to what should be awarded to successful plaintiffs. Without a predictable standard for courts to apply, courts may be reluctant to rule in favor of recognizing the data privacy and security rights.[124] With two types of monetary remedies available to courts to provide—restitution and damages—policymakers should consider which type of monetary remedy would be the most appropriate to include in data privacy and security legislation.[125]

[54] In weighing the two types of monetary remedies against each other, restitution would be ineffective because restitution is measured by the defendant's gain.[126] With a data breach, like Equifax experienced,[127] the business would not gain anything (Equifax lost money). However, with a data privacy violation, like Facebook experienced,[128] the business is posed to gain (Facebook profited from the improper dissemination of PI). Thus, restitution would not effectuate an individual's *security* protections—only an individual's *privacy* protections.[129] Further, restitution would not

[123] *Id.* at 686.

[124] *Id.* at 657.

[125] *See id.* at 672.

[126] *See id.* at 672. *See generally* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011) (stating that benefit-based liability enjoyed by the defendant corresponds to an observable loss on the part of the plaintiff).

[127] *Supra* Introduction ¶ 2.

[128] *Supra* Introduction, at ¶ 1.

[129] *See generally* Scholz, *supra* note 46 ("[U]nder section 13(b) of the Federal Trade Commission Act, the FTC is specifically authorized to apply restitutionary remedies in its

eliminate or reduce the calculation difficulty. For example, how would a court measure Facebook's gain from violating a user's privacy rights? The court could calculate the annual revenue per user and award this amount as restitution, but even for Facebook, this amount is too low to justify the cost of litigation, and serve as actual deterrence.[130] Alternatively, the court could order Facebook to calculate how much revenue or profit it made from the particular plaintiff's PI, but it is highly unlikely Facebook maintains the technological capability to track its revenue by each and every user. Therefore, restitution would not serve the goals of protecting individuals' rights to data privacy and security.

[55] Damages would be more effective in protecting an individual's rights because damages are assessed by the loss to the plaintiff.[131] Unlike restitution, damages can apply to both privacy and security violations.[132] In both examples above (Equifax and Facebook), the plaintiff loses something of value. However, as previously discussed, the loss to the plaintiff would be difficult to calculate. To solve for this difficulty, when a legislature elevates the intangible injury to an injury-in-fact,[133] policymakers can determine the extent of the harm and prescribe statutory damages

resolution of privacy and data protection matters, under the broad category of 'unfair or deceptive practices.'").

[130] *See, e.g.*, Facebook, Inc., *supra* note 102 (reporting an annual revenue per user of $34.86 for Facebook in 2018 in the U.S. and Canada).

[131] *See* Scholz, *supra* note 46, at 671–673.

[132] *See generally id.* (Assuming policymakers elevate the violation to an injury-in-fact, if a business violates an individual's privacy rights, then the individual (plaintiff) is injured. Likewise, if a business violates an individual's security rights, then the individual is injured. Unlike restitution—where a business would not gain from a data breach—since damages focus on the plaintiff's loss, both types of violations are redressable because both result in an injury.).

[133] *See supra* Part II.A.

accordingly.[134] Not prescribing damages creates a risk—the court, especially juries, could return a disproportionately low or high damage award.[135]

[56] In determining the damages, policymakers should consider the remedy's ability to deter violations and the proportionality of the remedy.[136] Existing data privacy laws may serve as a guide. BIPA provides for $1,000 or actual damages for negligent violations and $5,000 or actual damages for intentional or reckless violations.[137] CCPA provides for damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.[138]

[57] Therefore, to effectuate a limited PROA, policymakers must (i) elevate the violation of an individual's data privacy and security rights to an injury-in-fact; and (ii) prescribe statutory damages as the remedy.

IV. CONCLUSION

[58] In his passionate advocacy for the right to privacy, Justice Brandeis asserted, "[e]xperience should teach us to be most on our guard to protect

[134] *See Damages*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Statutory Damages").

[135] *See, e.g.*, Richard Gonzalez, *California Jury Awards $2 Billion to Couple in Roundup Weed Killer Cancer Trial*, NAT'L PUB. RADIO (May 13, 2019), https://www.npr.org/2019/05/13/723056453/california-jury-awards-2-billion-to-couple-in-roundup-weed-killer-cancer-trial [https://perma.cc/G4MX-R4CA] (discussing jury awards greater than $50 million for successful plaintiffs in tort litigation against Bayer alleging Roundup weed killer caused cancer).

[136] *See* Scholz, *supra* note 46, at 685; *see also* Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV 2, 28 (2020).

[137] 740 ILL. COMP. STAT. ANN. 14/20 (2020).

[138] CAL. CIV. CODE § 1798.150(a)(1)(A-C) (Deering 2020).

liberty when the Government's purposes are beneficent."[139] As technological advancements centralize, concentrate, and multiply PI, under the guise of public benefit and societal progression,[140] the Government is no longer the primary infringer of privacy and security rights that individuals need protection from—private businesses are more powerful and intrusive than they have ever been before.[141] As private businesses rationalize the collection, use, and sale of PI as beneficial, experience should teach us to be most on our guard to protect our individual liberties. For "[m]en born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty [rather] lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[142]

[59] For the foregoing reasons, comprehensive data privacy and security legislation should include a limited PROA. If policymakers provide for a limited PROA, the injury-in-fact requirement for standing should not pose a constitutional limitation to would-be plaintiffs so long as policymakers elevate the intangible injury. Lastly, damages for such violations should be prescribed by statute at an effective and proportionate level.

---

[139] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) ("If the Government becomes a lawbreaker, it breeds contempt for the law; it invites every man to become a law unto himself; it invites anarchy . . . to declare that the Government may commit crimes . . . to secure the conviction of a private criminal . . . would be terrible retribution.").

[140] *See, e.g.*, FACEBOOK http://about.fb.com/company-info/ [https://perma.cc/JH7L-KL6C] (2020) ("Give people the power to build communication and bring the world closer together.").

[141] *See generally* Louis Menand, *Why Do We Care So Much About Privacy?*, THE NEW YORKER (June 11, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy [https://perma.cc/46QS-A5PY] (describing how technological advancements have led to greater intrusions).

[142] *Olmstead*, 277 U.S. at 479.