
THE RUTGERS UNIVERSITY LAW REVIEW
VOLUME 73 | ISSUE 5 FALL 2021

THE IMPORTANCE OF A PRIVATE RIGHT OF ACTION IN FEDERAL BIOMETRIC PRIVACY LEGISLATION

by Andrew Serulneck

TABLE OF CONTENTS

INTRODUCTION

Technological advancement has always been accompanied by new risks of harm,[1] while society mitigates these threats through the establishment of corresponding rights and duties.[2] Examples abound: by

1. *See* Morissette v. United States, 342 U.S. 246, 253–54 (1952).
2. *See id.*; *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

exposing larger numbers of workers to more severe injuries, the industrial revolution begat the conceptualization of workplace safety laws that required higher precautions by employers.[3] Wide distribution of goods called for regulations to protect consumers.[4] Enhanced communications technologies of the late 19th and early 20th century caused legal scholars to develop a right to privacy.[5] As we are learning more and more with each passing day, the information age is also posing new threats that will require society to recognize new protections in law.

One such threat is materializing in the form of data collection. Given the enhanced capabilities of firms to collect data, combined with the proliferation and ubiquity of sensors to effectuate this absorption, new threats to informational privacy have arisen which demand new rights to be recognized and new duties imposed.[6] Firms with more information have always been more efficient than firms with less, but the information age has drastically increased the capacity of firms to learn about consumers.[7] As a result, we have become surrounded by devices that record every facet of our lives.[8] Worse yet, because these malfeasants are private enterprises and not governments actors, they cannot be constrained by the Constitution's usual mechanisms for combatting

3. *See Morissette*, 342 U.S. at 253–54.

4. Laura Nader, *Seegers Lecture: The Life of the Law – A Moving Story*, 36 VAL. UNIV. L. REV. 655, 656 (2002) ("In 1916, Justice Benjamin Cardozo, in *MacPherson v. Buick Motor Co.*, signaled the beginnings of a change from a *caveat emptor* society that places the burden of proof on the unsuspecting consumer to a world that places the burden on the manufacturer."); *see also* MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

5. Warren & Brandeis, *supra* note 2, at 195 ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person . . . [i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").

6. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 879–80 (2016) ("If billions of sensors filled with personal data fall outside of Fourth Amendment protections, a large-scale surveillance network will exist without constitutional limits."); *see also* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 479 (2019).

7. This business model that harvests data to predict and influence consumer behavior has broadly been termed "surveillance capitalism." *See generally* ZUBOFF, *supra* note 6.

8. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 556–58 (2016) ("As new efficiencies have pushed down the cost of sensors and new innovations have improved the communication capacities of low-power devices, the growth of these smart devices has dramatically expanded. . . . One can now buy a smart watch, drive a smart car, live in a smart home, and even drink from a smart cup that monitors the amount and type of liquids you drink. Wearable technology has revolutionized professional sports, personal fitness training, health monitoring, and has even been incorporated into maternity clothing to track fetal health. A culture of self-monitoring products under the concept of 'the Quantified Self' has encouraged cultural acceptance and spurred technological innovation.").

unwanted intrusion into our lives.[9] In theory, this should be unsettling,[10] but in practice there seems to be an unspoken consensus that unfettered access into the most intimate facets of our lives is a small price to pay for the modern conveniences these firms offer.[11]

Of course, not all information about a person is so sensitive or personal that its mishandling alone presents a threat of actual harm.[12] While not all uses of data generally are innocent or noble,[13] at the same time not all information warrants harsh consequences for data collectors if mishandled. For example, traditional data tends to be much more benign than biometrics, because there is a limit to how much harm can befall someone who has their bank pin stolen. For obvious reasons, the handling of biometric data entails a much more serious degree of potential harm, necessitating more strenuous monitoring and imposing an increased duty of care upon those firms that handle it. The perspective of our federal courts and legislature must evolve to recognize this distinction.[14]

As this note discusses at length, the handling of biometric information by its very nature entails more serious risks than when an

---

9. Ferguson, *supra* note 6, at 879–80.

10. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 61–76 (examining contemporary business models and corporate behaviors which "rarely breach any of the recognized principles of privacy and data protection law . . . include activity that is not exactly harmful, does not circumvent privacy settings, and does not technically exceed the purposes for which data were collected" but nonetheless "pushes against traditional social norms" and "exposes a rift between the norms [of those who develop new technologies] and those of the public at large . . . .").

11. *See* Caleb Garling, *Google Enters Homes with Purchase of Nest*, S.F. CHRON., Jan. 14, 2014, at D6 ("Palo Alto's Nest is a flagship brand in the burgeoning Internet of Things — a catchphrase for a wave of tech innovations that could turn once-mundane appliances like ovens, thermostats, microwaves, fridges and garage-door openers into a network of devices that communicate with each other."); Lucas Matney, *More than 100 Million Alexa Devices Have Been Sold*, TECHCRUNCH (Jan 4, 2019, 5:10 PM), https://techcrunch.com/2019/01/04/more-than-100-million-alexa-devices-have-been-sold/; Jordan Valinsky, *Amazon Reportedly Employs Thousands of People to Listen to Your Alexa Conversations*, CNN BUS. (Apr. 11, 2019, 2:38 PM), https://www.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html.

12. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) ("It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.").

13. *See* SETH STEPHENS-DAVIDOWITZ, EVERYBODY LIES 134–38 (2017) ("Data on the internet . . . can tell businesses which customers to avoid and which they can exploit.").

14. *See* Chaminda Hewage, *Stolen Fingerprints Could Spell the End of Biometric Security – Here's How to Save It*, CONVERSATION (Aug. 20, 2019, 8:06 AM), https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001 ("Traditional passwords are something you know. Biometric features are something you are.").

entity is entrusted with traditional data.[15] While someone may change, for example, their passwords, social media profile, license plate, credit card or social security number with relative ease, the same cannot be said for one's face, eyes, voice, or fingerprints.[16] Given the permanence of these risks, those who collect or use biometric data for any purpose should be viewed by our legal system with a much more powerful skepticism.[17]

Raising the stakes even further is that private firms have failed time and again to properly secure their traditional data from breaches.[18] Given this history, it is unlikely that they will be able to secure biometrics any more effectively moving forward without the proper incentives. Thus arises the question of what sort of regulatory framework is most likely to motivate firms to take appropriate measures to secure biometric data more effectively than they have secured traditional data. While it is beyond dispute that *some* regulation is necessary, the character of a prospective regulatory scheme is still up for debate.

Thankfully, state legislatures across the country have started to implement their own standards for handling biometric information and we can simply look to their example.[19] These laws, and the litigation that followed their passage, offer valuable lessons in terms of what effectively protects biometric privacy and what does not. Given the idiosyncrasies of the biometric data issue, a very specific cocktail of legislative fixes may be required from Congress.

The most essential component of this cocktail (and the subject of this note) is the private right of action. Again, given the frequency and permanence of data privacy violations, it is hopeless to expect the government alone to enforce these rights to the extent necessary. Private rights of action empower citizens to protect *themselves* by allowing plaintiffs to sue a private actor for violating a law meant to protect a plaintiff's rights as defined under a given statute. Traditionally, privatizing enforcement has ensured much stricter compliance with

15. *See* STEPHENS-DAVIDOWITZ, *supra* note 13, at 134–38; *see also* 740 ILL. COMP. STAT. 14/5(c) (2008) ("For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.").

16. *See* STEPHENS-DAVIDOWITZ, *supra* note 13, at 134–38; Hewage, *supra* note 14.

17. *See* 740 ILL. COMP. STAT. 14/5(c) (2008).

18. *See* IDENTITY THEFT RES. CTR., 2017 ANNUAL REPORT 8 (2017) ("The final number for of data breaches reported for 2017 was 1,579 . . . .").

19. CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020); 740 ILL. COMP. STAT. 14/1-14/99 (2008); WASH. REV. CODE §§ 19.375.010–19.375.900 (2017); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

regulatory schemes.[20] However, this potent regulatory tool is not without its critics. The Supreme Court has recently questioned the constitutionality of a private right of action in certain contexts,[21] and it's possible that the Court might not uphold a private right of action in certain data privacy cases even if Congress outlined one via statute.

Part I of this note will discuss the nature of the threats posed by collectors of biometric data and outline what is at stake if we fail to regulate its retention, collection, disclosure and destruction.[22] Part II of this note will discuss recent measures taken by state legislatures to ensure biometric data privacy. This discussion will highlight statutory provisions that have been successful, giving particular attention to the all-important private right of action. Part III of this note discusses the Supreme Court's most recent interpretation of standing in a data privacy context and, more specifically, the prospect that the Supreme Court would not grant private litigants standing to protect their biometric data privacy rights if Congress were to pass laws similar to what some states have recently enacted.

I. WHY BIOMETRIC DATA REQUIRES MORE AGGRESSIVE PROTECTION THAN STANDARD DATA

The most valuable commodity of the Information Age is data.[23] In this new era where knowledge is the ultimate power, information has actual monetary value because data itself enables its possessor to operate more efficiently and profitably.[24] For obvious reasons, firms in every industry stand to benefit enormously from obsessively absorbing as much of this new resource as they can.[25]

---

20. For example, in the case of short swing profits by insider traders, Section 16(b) of the Securities and Exchange Act of 1934 empowers private plaintiffs to sue for disgorgement of all profits by directors and major shareholders of a corporation who violate certain statutory restrictions. *See* Securities and Exchange Act of 1934 § 16(b), 15 U.S.C. §§ 78p(a)–(b); *see also* False Claims Act of 1986, 31 U.S.C. §§ 3729–3733 (1994); Fair Credit Reporting Act, 15 U.S.C. § 1681n (outlining civil liability for willful noncompliance); Cable Communications Policy Act, 47 U.S.C. § 551(f); J. Randy Beck, *The False Claims Act and the English Eradication of* Qui Tam *Legislation*, 78 N.C. L. REV. 539, 541, 566 (2000); *see also infra* note 109.

21. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

22. Wording taken from Illinois' Biometric Information Privacy Act. *See* 740 ILL. COMP. STAT. 14/15 (2008).

23. *The World's Most Valuable Resource is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

24. *See id.*

25. *See id.*

The data firms seek comprises literally every aspect of a human being's life.[26] Collecting this information is easy, since we now exist in a world surrounded by devices that record our every move.[27] Obviously this entails enormous concerns about an individual's privacy, and courts and legislatures at every level have sought to regulate the consumption and handling of consumer data.[28] While a small handful of state legislatures and courts have seen some degree of success in protecting peoples' data, many federal courts (including the Supreme Court of the United States) have been hesitant to find standing in data privacy cases where plaintiffs allege statutory harms alone, finding them to lack the requisite "concreteness" and "particularity" necessary to satisfy Article III of the United States Constitution.[29] They have also questioned the wisdom of allowing private litigants to bring suits to impose penalties on defendants for wrongs they see as being borne by the public at-large.[30]

Protecting biometric[31] data can be tricky. There are countless services, gadgets and appliances constantly recording and storing information concerning every facet of our lives.[32] Peddlers of this technology have claimed that this advancement was meant to make their products more attractive to consumers by making our information more secure[33] and our lives more convenient.[34] It remains unclear whether any of these purported justifications for recording biometrics have been achieved,[35] but what is certainly true is that, many firms have an enormous financial incentive to mine this data.[36] It is unclear whether these new biometric-reliant technologies actually have a net-positive impact on security, safety, or efficiency,[37] since paradoxically these same

26. *See* Ferguson, *supra* note 8.

27. *See* Ferguson, *supra* note 6.

28. *See* CAL. CIV. CODE §§ 1798.100-1798.199 (West 2021); 740 ILL. COMP. STAT. 14/1-14/99 (West 2008); WASH. REV. CODE. § 19.375 (West 2017); TEX. BUS. & COM. CODE ANN. § 503 (West 2017); Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (2019).

29. *E.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

30. *See id.* at 1550–54 (Thomas, J., concurring).

31. *See generally* Mark G. Milone, *Biometric Surveillance: Searching for Identity*, 57 BUS. LAW. 497, 497 n.1 (2001).

32. Ferguson, *supra* note 8, at 556–58 (2016).

33. *See* Tene & Polonetsky, *supra* note 10.

34. *See, e.g.*, *10 Ways Alexa Makes Life Easier for Prime Members*, PRIME INSIDER, https://www.amazon.com/primeinsider/top-alexa-tips (last visited July 15, 2021).

35. April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ (explaining that biometrics "are inherently public" and, thus, arguably less secure).

36. *See* ZUBOFF, *supra* note 6, at 480–81.

37. *See id.*

firms have failed to exercise care in protecting that data to such an extent that data breaches have become commonplace.[38]

Leaving aside the question of whether biometric-reliant technologies are effective or even necessary, the reality is that we have been asked to expose information intimately entwined with our personhood to theft from which we can never truly reclaim it.[39] That is why our laws must recognize a distinction between traditional data and biometric data. Traditional data[40] does not entail the same risk of permanent harm if it is mishandled (though there are many uses of traditional data that are considered by some to be "creepy").[41]

Biometric data, however, differs from traditional data.[42] Biometric data privacy is unique from traditional data because the harms that will result if this information falls into the wrong hands are potentially far worse.[43] While someone may change their social media profile, credit card or social security number with relative ease, the same cannot be said for one's face, eyes, voice, or fingerprints.[44] For instance, once someone else possesses your fingerprint (which can be stolen simply by analyzing a picture of your hand,[45] or using a "master print"[46]) no information that

38. *See* IDENTITY THEFT RES. CTR., *supra* note 18, at 8 ("The final number of data breaches reported for 2017 was 1,579.").

39. Hewage, *supra* note 14.

40. *See* STEPHENS-DAVIDOWITZ, *supra* note 13, at 4 ("[P]eople's search for information is, in itself, information . . . [t]he everyday act of typing a word or phrase into a compact, rectangular white box leaves a small trace of truth that, when multiplied by millions, eventually reveals profound realities.").

41. *See* Tene & Polonetsky, *supra* note 10, at 61 (examining contemporary business models and corporate behaviors that often comply with privacy laws and principles but nonetheless "push[] against traditional social norms").

42. *See* Jayshree Pandya, *Hacking Our Identity: The Emerging Threats From Biometric Technology*, FORBES (Mar. 9, 2019, 12:26 PM), https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/#45791f8d5682 ("Perhaps most importantly, the automation of human identity authentication raises fears about the possibility of a surveillance society . . . the way the digital data is produced, stored, compared and possibly linked to other information about the individual raise serious concerns for the blurring boundaries between privacy and security and security and surveillance.").

43. *See id*. ("Since human identity is central to the functioning of the human ecosystem, any emerging threat to its biometric indicators is a threat to human identity authentication—bringing complex security risks for the future of humanity."); *see also* STEPHENS-DAVIDOWITZ, *supra* note 13 ("Traditional passwords are something you know. Biometric features are something you are.").

44. *See* Pandya, *supra* note 42.

45. Olanrewaju Sodiq Olamide, *Why You Shouldn't Use Fingerprint/Touch ID and Face ID*, DIGNITED (July 30, 2019), https://www.dignited.com/49561/why-you-shouldnt-use-fingerprint-touch-id-and-face-id/.

46. *Id*. ("Master prints are fingerprints that have been engineered to match multiple patterns. With a 65% success rate, these master prints are able to unlock your device by capitalizing on the small size of your phone's fingerprint scanner — which only matches a

you have used that fingerprint to secure will ever be safe again. The law must recognize the increased risks associated with securing one type of data versus another. That is to say that the law much distinguish between information that is *about* us and information that *is* us.

This would not be the first time the law has had to respond to encroachments upon privacy by technological advancement.[47] Often times, these responses have called for recognizing changing realities and adopting our societal standards accordingly.[48] To that end, legislators must adopt more proactive tools to regulate biometric data collection and storage than they would with other less sensitive information by updating laws in lockstep with advances in technology.[49] The law must once again adapt to recognize harms where none existed before.[50] Given the aggressive nature of the potential harms stemming from the collection, storage and transfer of biometric data, these harms must be treated with more caution than the harms associated with standard data.

II. CURRENT BIOMETRIC PRIVACY LEGISLATION AT THE STATE LEVEL

In response to these threats that have emerged, there is momentum at the state level to introduce legislation to give people more control over their biometric identifiers.[51] At the time of this writing, four states had passed biometric privacy laws: Illinois, Texas, Washington, and

---

partial scan (rather than all the ridges) of your finger. This is why fingerprint sensors are fast, and at the same time, flawed.").

47. *See* Warren & Brandeis, *supra* note 2; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000). *But see, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011) (holding that "hypothetical, future injury" is not sufficient to establish Article III standing and therefore refraining from ruling on the merits of the data-breach issue).

48. *See also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992) (noting that Congress may "elevate[] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law"); *id.* at 580 (Kennedy, J., concurring in part) ("Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before . . . ."). *But see* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation.").

49. *See* ZUBOFF, *supra* note 6, at 480 ("So far US privacy laws have failed to keep pace with the march of instrumentarianism.").

50. *See* Cohen, *supra* note 47, at 1377 ("We must carve out protected zones of personal autonomy, so that productive expression and development can have room to flourish. We can do so—constitutionally—by creating a limited right against certain kinds of commercial collection and use of personally-identified information.").

51. *See* 740 ILL. COMP. STAT. 14 (2008); WASH. REV. CODE. § 19.375 (2017); TEX. BUS. & COM. CODE ANN. § 503 (West 2017); CAL. CIV. CODE §§ 1798.100-1798.199 (West 2020).

California.[52] These experiments at the state level can be analyzed to provide insight regarding what sorts of provisions should be included in federal legislation.

There have been two key provisions of effective biometric regulation at the state level. First, statutes have placed the burden on private entities that collect biometric information to give adequate notice and obtain informed consent from the subject. Second, the notice and informed consent requirements are enforced through a private cause of action. Without both of these provisions, biometric privacy legislation is practically toothless.

A. *The Importance of Notice and Informed Consent*

Notice and informed consent are crucial to empower individuals to control their data.[53] These concepts go hand-in-hand, because without notice there cannot be valid consent. Notice, in the context of data privacy regulations, is meant to force a collector of personally identifiable information ("PII") to make the subject of that PII aware of what data it proposes to collect and how it proposes to use that data.[54] Assuming notice is adequate, the subject of that data must invariably make a choice to give or deny consent.[55] The subject is thereby exercising the agency and autonomy that would otherwise have been denied to them. Given the countless ways that biometric data can be collected without the subject ever knowing, any statute serious about protecting a right to biometric privacy must require entities to give adequate notice and obtain informed consent from their subject.[56]

---

52. *See* 740 ILL. COMP. STAT. 14 (2008); WASH. REV. CODE. § 19.375 (2017); TEX. BUS. & COM. CODE ANN. § 503 (West 2017); CAL. CIV. CODE §§ 1798.100-1798.199 (West 2020).

53. *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. L. REV. 559, 561 (2018).

54. Thomas B. Norton, Note, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 184 (2016).

55. *See id.*

56. *See, e.g.*, Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (Dec. 30, 2014, 6:43 AM), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands; Ian Morris, *Samsung Galaxy S8 Iris Scanner Hacked in Three Simple Steps*, FORBES (May 23, 2017, 11:14 AM), https://www.forbes.com/sites/ianmorris/2017/05/23/samsung-galaxy-s8-iris-scanner-hacked-in-three-simple-steps/#24d3617ccba8; Hewage, *supra* note 14; Colm Gorey, *Voice Recognition Tech Hacked with Voice-Morphing Tool*, SILICON REPUBLIC (Sept. 28, 2015), https://www.siliconrepublic.com/enterprise/voice-recognition-security-easily-hacked; Andy Greenberg, *Hackers Say They've Broken Face ID a Week After iPhone X Release*, WIRED (Nov. 12, 2017, 6:44 PM), https://www.wired.com/story/hackers-say-broke-face-id-security/.

In a world saturated with cameras and sensors, it is virtually impossible to hide one's biometrics from being absorbed coincidentally.[57] For this reason, biometric privacy statutes in Illinois, Texas, Washington and California have all included notice and informed consent provisions in their language.[58] Notice provisions make these statutes effective because by surreptitiously (though perhaps innocently) collecting an individual's biometrics, a private entity commits a statutory violation sufficient to sustain a lawsuit.[59] Unfortunately, even with strict notice and informed consent provisions, biometric privacy legislation can still be rendered toothless without adequate enforcement mechanisms in place.

B. *The Importance of a Private Right of Action*

This brings us to the private right of action. Provisions for private enforcement, coupled with provisions outlining requirements of notice and consent, are by far the most crucial components of any prospective biometric privacy legislation. The effect of strict notice and consent requirements working in tandem with a private right of action is a weapon uniquely suited for the fight against tech firms that encroach upon privacy rights.

The advantages the private right of action confers are difficult to replicate by other means. That is precisely why so many federal statutes meant to protect consumers utilize the private right of action.[60] By allowing for private cause of action in a statute, legislatures encourage aggressive compliance and efficiency.[61] Without this mechanism in place, any rights outlined by a legislature, whether local, state or federal, are

57. *See* Ferguson, *supra* note 6.

58. *See* Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, BLOOMBERG L. (Oct. 12, 2017, 5:44 PM), https://news.bloomberglaw.com/privacy-and-data-security/washingtons-new-biometric-privacy-statute-and-how-it-compares-to-illinois-and-texas-law; *see also* statutes cited at *supra* note 52.

59. *See, e.g.*, Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (stating that, by disregarding the notice and consent requirement in Illinois' Biometric Informational Privacy Act, "the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the . . . legislature sought to prevent is then realized."); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019) ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief . . . .").

60. *See* False Claims Act, 31 U.S.C. § 3730(b); Fair Credit Reporting Act, § 616, 15 U.S.C. § 1681n (outlining civil liability for willful noncompliance); Cable Communications Policy Act, 47 U.S.C. § 551(f).

61. Matthew C. Stephenson, *Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies*, 91 VA. L. REV. 93, 106–07 (2005).

unlikely to be enforced to such an extent that will effectively counterbalance the aggressive collection tactics of so-called (and aptly labeled) surveillance capitalists.[62]

A private right of action accomplishes this in several ways. First, a private right of action facilitates aggressive enforcement of a statute, while preventing government agencies from, for whatever reason, underenforcing regulations.[63] This benefit of private enforcement is crucial to any efforts to regulate the handling of biometric information. As this article has already discussed, large tech firms have enormous political influence, as well as an interest in avoiding liability for biometric privacy violations. Outlining a cause of action for private citizens acts as a check on government agencies that may be incentivized by political pressure, budgetary constraints or outright laziness to exercise discretion to underenforce the law while informational privacy rights are being violated.[64]

Second, private enforcement of public laws relieves the government of many of the costs associated with enforcement, facilitating a more efficient regulatory scheme for both the government agencies who oversee enforcement and the private citizens they serve.[65] When applied in conjunction with notice and consent provisions (or any form of required disclosure),[66] a private right of action can serve as a more reliable mechanism for enforcement because private parties are often better positioned than an attorney general or other government agency to monitor compliance.[67] Furthermore, by delegating the responsibility of policing certain types of statutory violations to well-informed private plaintiffs with sufficient incentives to sue, government agencies can focus

62. ZUBOFF, *supra* note 6, at 479 ("The facts of surveillance capitalism's dominance of the division of learning, the unrepentant momentum of its dispossession cycle, the institutionalization of its means of behavior modification, the convergence of these with the requirements of social participation, and the manufacture of prediction products for trade in behavioral futures markets are de facto evidence of a new condition that has not been tamed by law.").

63. Stephenson, *supra* note 61, at 110–12.

64. *Id*.

65. *See id*. at 107–08 ("By deputizing hundreds or thousands of individual citizens and interest groups to act as private attorneys general, citizen-suit provisions (and other forms of express or implied private rights of action) can dramatically increase the social resources devoted to law enforcement, thus complementing government enforcement efforts.").

66. *See* Securities and Exchange Act of 1934 § 16(b), 15 U.S.C. § 78p(b) (empowering private plaintiffs who own securities of a corporation to sue for disgorgement of all profits by directors and major shareholders of a corporation who obtain 'short-swing' profits by committing statutory violations); 15 U.S.C. § 78p(a) (outlining disclosure requirements for transactions of directors, officers, and principal stockholders who may seek to obtain short-swing profits through statutory violations).

67. *See* Stephenson, *supra* note 61, at 108.

on prosecuting violations where the government has a more generalized interest in the litigation.[68]

Considering the ease and speed with which violations of this sort can be committed, it would be ridiculous for us to expect any government agency to monitor every face, eyeball or fingerprint that was scanned without permission. While the private right of action is a controversial tool, it is particularly useful when seeking to facilitate strict and efficient compliance with consumer protection laws where constant government oversight is unrealistic.[69]

C. *The Effectiveness of the Private Right of Action in a Biometric Privacy Context*

To illustrate the utility of enforcing notice and consent provisions with a private right of action in a biometric privacy context, we can look to the Illinois Supreme Court's decision in *Rosenbach v. Six Flags*.[70] There, a parent of a minor (Stacy Rosenbach) sued Six Flags Great America (an amusement park) on behalf of her son after the defendant failed to obtain her notice and consent before scanning and storing her child's fingerprint in their system.[71] This action, Rosenbach alleged, was a violation of Illinois' Biometric Information Privacy Act.[72]

The Illinois Supreme Court reviewed the case *de novo* and reversed an appellate court's dismissal of Rosenbach's claim.[73] Regarding the notice and consent requirements, the court held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief . . . ."[74] The state's highest court reasoned that the violation of statutory rights alone was sufficient to confer standing, and that to require plaintiffs to meet a higher threshold would render the law pointless in light of the law's purported purpose to *proactively* protect citizens from the unique and unpredictable consequences of biometric technology which are not "fully

68. *See* Barry Boyer & Errol Meidinger, *Privatizing Regulatory Enforcement: A Preliminary Assessment of Citizen Suits Under Federal Environmental Laws*, 34 BUFF. L. REV. 833, 837–38 (1985).

69. For example, if the statutory provision in *Spokeo v. Robins* "created a private duty owed personally to Robins to protect his information[,]" Justice Thomas suggested that a violation of that duty should satisfy the injury requirement for standing and pave the way for private rights of action. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1553–54 (2016) (Thomas, J., concurring).

70. *See* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

71. *Id.* at 1200–01.

72. *Id.* at 1201–02.

73. *Id.* at 1202, 1207.

74. *Id.* at 1207.

known" at this time.[75] This can only be achieved by imposing safeguards to ensure that biometric identifiers are protected before they can be compromised[76] and imposing a substantial potential liability upon private entities for violations, "whether or not actual damages, beyond violation of the law's provisions [demanding proper notice and consent] can be shown."[77]

Through this holding, the *Rosenbach* court exercised its authority in the precise way that the state legislature had intended. As the Supreme Court of Illinois phrased so eloquently:

> The strategy adopted by the [Illinois] General Assembly through enactment of the Act is to try to head off such problems before they occur. It does this in two ways. The first is by imposing safeguards to insure [sic] that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised. The second is by subjecting private entities who fail to follow the statute's requirements to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses "for each violation" of the law whether or not actual damages, beyond violation of the law's provisions, can be shown.[78]

Crucially, the court did not stop there. Indeed, "the procedural protections in BIPA 'are particularly crucial in our digital world' because '[w]hen a private entity fails to adhere to the statutory procedures … the right of the individual to maintain his or her biometric privacy vanishes into thin air.'"[79] The court made a point to highlight the apparent intent of the Illinois Assembly in light of the fact that they chose to enforce the notice and consent provisions through a private right of action:

> The second of these two aspects of the law is as integral to implementation of the legislature's objectives as the first . . . [i]t is clear that the legislature intended for this provision to have substantial force. When private entities face liability for failure to comply with the law's requirements without requiring affected individuals or customers to show some injury beyond violation of

75. *Id.* at 1206–07.
76. *Id.*
77. *Id.* at 1207.
78. *Id.* at 1206–07.
79. Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019) (quoting *Rosenbach*, 129 N.E.3d at 1206).

> their statutory rights, those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone. Compliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law. To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to [BIPA's] preventative and deterrent purposes.[80]

As the Supreme Court of Illinois lays out above, the combination of notice and consent with a private right of action is a powerful legal tool to protect the biometric data rights of Illinoisans. Unfortunately, there are problems with leaving this issue to the states.

D. *Shortcomings of the 'Patchwork' Approach*

To be sure, most of the time there is nothing wrong with claims being brought exclusively in state courts. It is not uncommon for state courts to have a lower threshold for standing than federal courts.[81] However, this means that in the context of biometric data privacy, state legislatures will presumably develop their own biometric privacy laws, which state and federal courts will be responsible for interpreting one at a time over the course of many years. Several developments in biometric privacy laws at the state level now necessitate a federal response.

Outside of the courts, state legislatures seem to be developing cases of cold feet.[82] The current trend at the state level is that legislatures have become less focused on empowering consumers and more focused on protecting potential defendants.[83] Since Illinois chose to address biometric privacy in 2008, Texas, Washington and California have passed

---

80. *Rosenbach*, 129 N.E.3d at 1207.

81. Christopher M. Mason et al., *Yet Another Thing to Worry About: The Evolving Law of Standing in State Courts When Federal Standing Is Lacking*, NIXON PEABODY (Apr. 13, 2020), https://www.nixonpeabody.com/en/ideas/articles/2020/04/13/evolving-law-of-standing-in-state-courts-when-federal-standing-is-lacking.

82. *See* Danny Thakkar, *Biometric Regulations in the U.S. States: The State of Play*, BAYOMETRIC, https://www.bayometric.com/biometric-regulations-us-states/ (last visited Aug. 5, 2021).

83. *See id.* ("While privacy attorneys call it a weaker law than its Illinois counterpart, corporate advocates suggest that Washington's BIPA is more realistic and will protect both consumers as well as innovations.").

biometric privacy laws that lack essential features that made BIPA effective in the first place.[84]

Biometric privacy laws in Texas and Washington are particularly toothless with too many exceptions for the laws to be effective. For example, when Illinois passed BIPA in 2008, the statute's definition of "biometric identifier" specified that this was a record of "hand or face geometry."[85] This broad definition exposed many large tech firms to class-action tort liability for invasions of privacy.[86] By the time Washington enacted its biometric privacy law nine years later, their definition of biometric identifier[87] was much more vague and expressly excluded "a physical or digital photograph, video or audio recording or data generated therefrom . . . ."[88] Texas and Washington's biometric privacy acts limit the scope of their laws to a "commercial purpose," contain less stringent notice and consent requirements; do not allow for a private right of action; place strict limits on the damages that may be sought; and permit the sale of biometric identifiers under "enumerated circumstances."[89] Furthermore, Washington's biometric privacy laws "permit[] disclosure [of biometric data to third parties] under a significantly broader set of circumstances" than the privacy laws that came before it.[90] Moreover, BIPA is still the only state statute to offer a private cause of action for violations, while its counterparts in Texas and Washington offer nothing of the sort, forcing citizens to rely solely on the states' attorneys general to enforce the provisions.[91]

Ideally, federal biometric privacy legislation could address each of these shortcomings inherent of a patchwork regulatory regime. As communication and commerce across state lines have intensified in the United States, the need for greater uniformity of law on particular subjects has grown.[92] Out of this necessity, federal laws in these areas (transportation, communication and commerce) have been widely embraced.[93] When it comes to biometrics, the sheer volume, speed and reticence of data collection today makes it unlikely that a single federal

84. *See* Tumeh, *supra* note 58; CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020).

85. 740 ILL. COMP. STAT. 14/10 (2008).

86. Nicole O., *Biometrics Laws and Privacy Policies*, PRIVACYPOLICIES, https://www.privacypolicies.com/blog/privacy-policy-biometrics-laws/#Laws_Regulating_Biometrics_Use (last visited Aug. 6, 2021).

87. *See* WASH. REV. CODE § 19.375.010 (West 2017).

88. *Id.*

89. *Id.*; Tumeh, *supra* note 58.

90. Tumeh, *supra* note 58.

91. *See id.*

92. *See Uniform Laws*, LEGAL INFO. INST., https://www.law.cornell.edu/uniform (last visited Aug. 6, 2021).

93. *See* Securities Act of 1933, 15 U.S.C. § 77a (1933); Securities Exchange Act of 1934, 15 U.S.C. § 78a (1934); Federal Communications Act, 47 U.S.C. § 151 (1934).

agency alone could ensure compliance with such a law. Whereas under normal circumstances a private right of action would be a natural solution to this problem, the Supreme Court's recent iteration of standing requirements in data privacy cases outlined in *Spokeo, Inc. v. Robins* may have unnecessarily precluded Congress from utilizing the private right of action as a tool to enforce data privacy regulations.[94]

III. HOW *SPOKEO* MAY HAVE DOOMED THE PRIVATE RIGHT OF ACTION IN PROSPECTIVE FEDERAL DATA PRIVACY LEGISLATION

Spokeo, Inc. v. Robins [95] was a seemingly mundane case that resolved a compliance issue regarding the burden placed on consumer reporting agencies under the Fair Credit Reporting Act.[96] Spokeo, Inc. operates a website featuring a "people search engine" with which its users can obtain in-depth consumer reports on individual persons.[97] The plaintiff, Thomas Robins, alleged that his employment prospects had been harmed when Spokeo's website displayed false information about him and sued under relevant provisions of the FCRA.[98] The FCRA requires consumer reporting agencies, whenever preparing a consumer report, to follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.[99] To promote adherence to the Act's procedural requirements, Congress granted adversely affected consumers a right to sue noncomplying reporting agencies for damages.[100]

Ultimately, the Supreme Court took no position regarding whether the procedural violations alleged in *Spokeo* entailed a degree of risk sufficient to have standing and remanded the case back to the Ninth Circuit to determine whether they comported with the Constitution's "concreteness" requirement.[101] *Spokeo* only dealt with a specific form of "traditional" data, the factors analyzed to determine one's creditworthiness.[102] However, the decision has been interpreted to apply

94. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
95. *Id.*
96. *See id.*
97. *Id.* at 1544.
98. Spokeo's profile of him falsely stated that he worked in a professional field, had a graduate degree, was a married parent, exaggerated his net worth, and included a false age and profile photograph. *See id.*
99. *Id.* at 1554 (Ginsburg, J., dissenting).
100. *Id.*
101. *Id.* at 1550 (majority opinion).
102. *See id.* at 1545.

to a wide range of data types in a variety of scenarios.[103] It is now unclear when a plaintiff has standing to sue for mishandling or abuse of their data, even if Congress has afforded them a statutory right to do so.

A. *What Is "Standing?"*

At this point it may be useful to discuss what "standing" is and why it exists to better understand why Congress may run into problems when or if they were to try to define an interest in biometric privacy that can support a private cause of action. The structure of the Constitution limits the authority of each branch of the Federal Government. To this end, it vests Congress with enumerated "legislative Powers,"[104] the President with "[t]he executive Power,"[105] and the courts with "[t]he judicial Power of the United States."[106] While Article III of the Constitution does not fully explain what is meant by "[t]he judicial Power of the United States,"[107] it specifies that this power extends only to "cases" and "controversies."[108]

"Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy."[109] The doctrine evolved to ensure that federal courts do not exceed their authority[110] by limiting the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong.[111] In so doing, the judicial branch is prevented from encroaching upon the powers of the political branches.[112]

The constitutional minimum of standing to sue consists of three elements: the plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.[113] To establish injury in fact, a plaintiff must show that he or she suffered an invasion

103. *See* Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 495, 495-506 (2018) (analyzing the impact of Spokeo on data privacy cases in federal courts).
104. U.S. CONST. art. I, § 1.
105. U.S. CONST. art. II, § 1, cl. 1.
106. U.S. CONST. art. III, § 1.
107. *Id.*
108. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546–47 (2016) (citing U.S. CONST. art. III, § 2).
109. *Id.* at 1547.
110. Raines v. Byrd, 521 U.S. 811, 820 (1997).
111. *See* Warth v. Seldin, 422 U.S. 490, 498–99 (1975).
112. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).
113. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

of a legally protected interest that is "concrete,"[114] "particularized,"[115] and "actual or imminent, not conjectural or hypothetical."[116] While a concrete injury must be "real" in the sense that it is not "abstract," that does not mean that the injury must necessarily be "tangible."[117] Moreover, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[118] However, even where Congress exercises that power to define new harms through statutes, Article III standing still requires a concrete injury even in the context of a statutory violation.[119]

B. *Standing Requirements in a Data Privacy Context*

In their most recent reiteration of what is required to establish standing under Article III in a data privacy context, the *Spokeo* Court remanded the case back down to the Ninth Circuit because their standing analysis was 'incomplete,' addressing only the 'particularization' requirement, but not the 'concreteness' of Robins' harms in determining whether or not Robins had alleged a legally cognizable injury in fact.[120]

---

114. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) ("A 'concrete' injury must be '*de facto*'; that is, it must actually exist. When we have used the adjective 'concrete,' we have meant to convey the usual meaning of the term – 'real,' and not 'abstract.' . . . 'Concrete' is not, however, necessarily synonymous with 'tangible.'") (first quoting BLACK'S LAW DICTIONARY 479 (9th ed. 2009); then quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 472 (1971); RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 305 (1967)).

115. *Id.* ("For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way."); *see also* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, 454 U.S. 464, 472 (1982) ("[standing] requires the party who invokes the court's authority to 'show that he personally has suffered some actual or threatened injury . . . .'") (quoting Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91, 99 (1979)).

116. *Spokeo, Inc.*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560).

117. *Spokeo, Inc.*, 136 S. Ct. at 1549 ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete."); s*ee also id.* at 1549 (first citing Fed. Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998)) ("[C]onfirming that a group of voters' 'inability to obtain information' that Congress had decided to make public is a sufficient injury in fact to satisfy Article III."); and then citing Pub. Citizen v. U.S. Dep't of Just., 491 U.S. 440, 449 (1989) ("[H]olding that two advocacy organizations' failure to obtain information subject to disclosure under the Federal Advisory Committee Act 'constitutes a sufficiently distinct injury to provide standing to sue.'").

118. *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring).

119. *Spokeo, Inc.*, 136 S. Ct. at 1547–48 ("Injury in fact is a constitutional requirement, and '[i]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue a plaintiff who would not otherwise have standing.'"); *see also id.* at 1549

120. *Spokeo, Inc.*, 136 S. Ct. at 1550 ("Because the Ninth Circuit failed to fully appreciate the distinction between concreteness and particularization, its standing analysis was incomplete. It did not address the question framed by our discussion, namely, whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet

Ultimately, the Court took no position as to whether Robins adequately alleged a concrete injury pursuant to Article III.[121] Even so, the effects of their hesitation have already reverberated down to lower courts.

In his concurrence, Justice Thomas shed some additional light on the Court's reasoning, delving into the difference between bringing suit to enforce a private right versus bringing suit to enforce a public right at common law,[122] and how this background continues to influence the Court's conception of standing in a data privacy context.[123]

> In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded. Thus, when one man placed his foot on another's property, the property owner needed to show nothing more to establish a traditional case or controversy . . . Common-law courts, however, have required a further showing of injury for violations of "public rights"—rights that involve duties owed "to the whole community, considered as a community, in its social aggregate capacity." Generally, only the government had the authority to vindicate a harm borne by the public at large, such as the violation of the criminal laws. Even in limited cases where private plaintiffs could bring a claim for the violation of public rights, they had to allege that the violation caused them "some extraordinary damage, beyond the rest of the [community]."[124]

It was this distinction between public and private rights that, in the majority's view, restricted the Court's jurisdiction over the matter in *Spokeo*. As Justice Thomas states, "[t]he Fair Credit Reporting Act creates a series of regulatory duties. Robins has no standing to sue Spokeo, in his own name, for violations of the duties that Spokeo owes to the public collectively, absent some showing that he has suffered concrete and particular harm."[125]

---

the concreteness requirement."); *see also id.* at 1549 ("[T]he violation of a procedural right granted by statute can be sufficient in *some* circumstances to constitute injury in fact . . . .") (emphasis added).

121. *See id.*

122. *See id.* (Thomas, J., concurring) ("Common-law courts more readily entertained suits from private plaintiffs who alleged a violation of their own rights, in contrast to private plaintiffs who asserted claims vindicating public rights. Those limitations persist in modern standing doctrine.").

123. *See id.* at 1550–54 ("These differences between legal claims brought by private plaintiffs for the violation of public and private rights underlie modern standing doctrine and explain the Court's description of the injury-in-fact requirement.").

124. *Id.* at 1551 (quoting 3 WILLIAM BLACKSTONE, COMMENTARIES *2).

125. *Id.* at 1553.

It is unclear why Justice Thomas felt that drawing this distinction between private and public rights was so important in this context. The basis for the majority's opinion, with which Thomas concurred, was that if plaintiffs were allowed to sue for harms they shared with the public, then that would be allowing private individuals to hijack the judicial branch and infringe upon the enforcement prerogatives of the executive branch.[126] However, this was a suit between two private parties, and as Thomas admits in his concurrence, "where one private party has alleged that another private party violated his private rights, there is generally no danger that the private party's suit is an impermissible attempt to police the activity of the political branches or, more broadly, that the [l]egislative [b]ranch has impermissibly delegated law enforcement authority from the executive to a private individual."[127]

Justice Ginsburg in her dissent justifiably pushes back against this reasoning, clarifying that "Thomas Robins instituted suit against Spokeo, Inc., alleging that Spokeo was a reporting agency governed by the FCRA, and that Spokeo maintains on its Web site an inaccurate consumer report about [Thomas] Robins."[128] Even if Robins was bringing the suit against Spokeo to enforce rights Spokeo (by virtue of a statute passed by Congress) owed to the public at large, the FCRA allows private litigants to sue defendants for statutory damages.[129] This would hardly be the only scenario in which private individuals were permitted (or even encouraged) by the federal government to do this.[130]

---

126. *See id.* at 1552–53.

127. *Id.* at 1553 (citing F. Andrew Hessick, *Standing, Injury in Facts, and Private Rights*, CORNELL L. REV. 275, 317–21 (2008)).

128. *Id.* at 1554 (Ginsburg, J., dissenting).

129. *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681(o)–(n).

130. *See* J. Randy Beck, *The False Claims Act and the English Eradication of* Qui Tam *Legislation*, 78 N.C. L. REV. 539, 566 (2000) (detailing the long history of *qui tam* suits in English and American jurisprudence, a form of litigation with roots in Roman as well as Anglo-Saxon law). The name "*qui tam*" is a shortened form of the Latin phrase "*qui tam pro domino rege quam pro si ipso in hac parte sequitur*," which translates to "[w]ho sues on behalf of the King as well as for himself." *Id.* at 541 n.3 (citing BLACK'S LAW DICTIONARY 1251 (6th ed. 1990)). The most recent codification of *qui tam* lawsuits was in 1986, when the United States Congress amended the False Claims Act (FCA) to more strongly encourage private citizens to bring an action on behalf of the government for recovery of a statutory penalty. *Id.* at 541 ("A *qui tam* statute permits a private citizen to bring an action on behalf of the government for recovery of a statutory penalty. The person who pursues the action . . . receives a portion of any amount recovered on the government's behalf. Thus, *qui tam* statutes privatize government litigation, permitting the private informer to sue for the government on a contingent-fee basis."). *Qui tam* suits are hardly some obscure legal mechanism. "[*Q*]*ui tam* statutes have been on the books since the first Congress and the FCA has contained a *qui tam* provision since the Civil War," although these suits saw a major surge in popularity following "the generous bounty offered to informers" under the 1986 amendment to the FCA. *Id.* at 541–42. Furthermore, the constitutionality of *qui tam* statutes was upheld by the Supreme Court in *Vermont Agency of Natural Resources v.*

While Justice Thomas' summary of the standing requirements of common law courts is generally true,[131] it conveniently overlooks any exceptions the Court has made when interpreting modern laws.[132] In other words, contrary to what you may find in the Justice Alito's majority's opinion or Justice Thompson's concurrence, private litigants have often been allowed—or even incentivized—to bring suits to enforce rights that defendants owe to the public, as long as those plaintiffs also had an interest in the outcome of the litigation.[133]

In her dissent, Justice Ginsburg asserted that the Court was wrong to remand the case to the Ninth Circuit[134] to determine whether Robins' alleged harm was "concrete."[135] Justice Ginsburg argued that far from raising a generalized grievance that no more interests Robins than it would any other member of the public, Robins was seeking redress "for

---

United States ex rel. Stevens, where the Court held that the injury-in fact sustained by the United States was sufficient to confer Article III standing on a *qui tam* plaintiff. *Id.* at 546–47. Given this background, Justice Thomas' criticism of private litigants suing to enforce private and public rights simultaneously is curious.

131. *See Spokeo*, 136 S. Ct. at 1551–52 (Thomas, J., dissenting).

132. *See* Reliance Elec. Co. v. Emerson Elec. Co., 404 U.S. 418, 422, *rehearing denied*, 405 U.S. 969 (1972) (quoting Bershad v. McDonough, 428 F.2d 693, 696 (7th Cir. 1970)) (explaining the Court's more lax standing requirements in the context of derivative suits brought under Section 16(b) of the Securities and Exchange Act of 1934) ("[T]he only method Congress deemed effective to curb the evils of insider trading was a flat rule taking the profits out of a class of transactions in which the possibility of abuse was believed to be intolerably great . . . [i]n order to achieve its goals, Congress chose a relatively arbitrary rule capable of easy administration. The objective standard of Section 16(b) imposes strict liability upon substantially all transactions occurring within the statutory time period, regardless of the intent of the insider or the existence of actual speculation. This approach maximized the ability of the rule to eradicate speculative abuses by reducing difficulties in proof. Such arbitrary and sweeping coverage was deemed necessary to insure the optimum prophylactic effect.") (internal quotation marks omitted); Securities and Exchange Act of 1934, § 16(b), 15 U.S.C. § 78p(a) (2011); False Claims Act of 1986, 31 U.S.C. §§ 3729–33 (1994); Fair Credit Reporting Act, 15 U.S.C. § 1681n (outlining civil liability for willful noncompliance); Cable Communications Policy Act, 47 U.S.C. § 551(f); J. Randy Beck, *supra* note 130, at 566. *But see* Donoghue v. Bulldog Invs. Gen. P'ship, 696 F.3d 170, 177 (2d Cir. 2012), *cert. denied*, 569 U.S. 994 (2013); *see also* Phillip Goldstein, *Section 16(B)—If at First You Don't Succeed . . .*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 1, 2017), https://corpgov.law.harvard.edu/2017/03/01/section-16b-if-at-first-you-dont-succeed/#2b (criticizing the standing analysis which has been endorsed by the federal courts in a Section 16(b) context as unconstitutional and speculating that the Supreme Court's holding in *Spokeo* may call the constitutionality of 16(b) derivative suits into question).

133. *See Spokeo*, 136 S. Ct. at 1556 (Ginsburg, J., dissenting)*; see also* Vermont Agency of Nat. Res. v. United States *ex rel* Stevens, 529 U.S. 765, 772 (2000).

134. It should be noted that the Ninth Circuit held that Robins' injuries satisfied the concreteness requirement. *See* Robins v. Spokeo, Inc., 867 F.3d 1108, 1118 (9th Cir. 2017).

135. *See Spokeo, Inc.*, 136 S. Ct. at 1555 (Ginsburg, J., dissenting) ("I part ways with the Court, however, on the necessity of a remand to determine whether Robins' particularized injury was 'concrete.'").

Spokeo's spread of misinformation specifically about him."[136] This misinformation, she concluded, was far from a "bare" procedural violation absent any concrete harm.[137] Misinformation about "his education, family situation, and economic status . . . could affect his fortune in the job market" [138] by "creating the erroneous impression that he was overqualified for the work he was seeking, that he might be unwilling to relocate for a job due to family commitments, or that his salary demands would exceed what prospective employers were prepared to offer him."[139]

C. *Impact of* Spokeo *on Private Rights of Action to Enforce Statutory Harms*

By unnecessarily remanding *Spokeo*, the Supreme Court created a gulf of legal uncertainty. As a result of this lack of clarity, there now exists a circuit split among lower courts as to when exactly a plaintiff has standing to sue for statutory harms.[140] On the one hand, many circuit courts have taken *Spokeo* as their cue to deny standing to plaintiffs who cannot show further harm beyond mere statutory violations, even when the law confers a private right of action upon prospective plaintiffs.[141] Other circuit court judges have interpreted Article III as granting plaintiffs the right to bring those types of suits where the statute does provide for a private right of action.[142]

---

136. *Id.* at 1555.

137. *See id.* at 1556.

138. *Id.*

139. *Id.* (citing Brief for Restitution and Remedies Scholars et al. as Amici Curiae in Support of Respondent at 35, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339)).

140. *See* Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 495, 499 (2018).

141. *See* Strubel v. Comenity Bank, 842 F.3d 181, 185 (2d Cir. 2016) (holding that an alleged violation of the Truth in Lending Act was not sufficient, on its own, to establish standing if the plaintiff could not demonstrate further harm); Crupar-Weinmann v. Paris Baguette Am. Inc., 861 F.3d 76, 77 (2d Cir. 2017) (holding that a plaintiff did not have standing in a suit against a defendant who printed a credit card expiration date on a receipt that was not truncated in violation of the Fair and Accurate Credit Transactions Act); Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 727 (7th Cir. 2016); Braitberg v. Charter Comm. Inc., 836 F.3d 925, 930 (8th Cir. 2016) (holding that a plaintiff did not have standing in a putative class action against a cable television provider who retained personally identifiable information of its customers after they had cancelled their subscription and after that information was no longer needed to provide services or collect payments in violation of the Communications Protection Act because the plaintiff had merely alleged a "bare procedural violation, divorced from any concrete harm"); Hancock v. Urban Outfitters Inc., 830 F.3d 511, 514–15 (D.C. Cir. 2016) (holding that a defendant requesting consumers' ZIP codes in violation of the Consumer Identification Information Act did not give a plaintiff standing).

142. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that the injury-in-fact requirement necessary to have standing may be established by "a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future

One side, consisting of the Second, Seventh, Eighth, and D.C. Circuits, has ruled that "even where Congress has accorded procedural rights to protect a concrete interest, a plaintiff may fail to demonstrate concrete injury where violation of the procedure at issue presents no material risk of harm to that underlying interest."[143] When it comes time to decide what constitutes a material risk and what does not, judges in these circuits have argued that statutory violations are insufficient on their own.[144] The other side of this circuit split, comprised of the Third, Ninth and Eleventh Circuits, has interpreted *Spokeo* to mean that there are circumstances under which procedural violations of a statute are sufficient injuries-in-fact for a plaintiff to establish standing.[145]

Clouding the issue further, when it comes to data breaches (as opposed to a defendant merely violating a statute meant to regulate the handling of data), the rule set down in *Clapper* persists, specifically that in order to have standing to sue because of the looming threat of future harm, that harm must be "certainly impending."[146] However, a growing portion of the federal appellate courts have begun to classify a "substantial risk of identity theft" as a result of a defendant's actions as being sufficient to establish standing.[147]

In fairness, the Supreme Court probably did not intend for their holding in *Spokeo* to be interpreted so broadly as to apply to all data privacy cases. Unfortunately, absent clarification from the Court or guidance from Congress, that's exactly what we can expect. The *Spokeo* Court could have added clarity by defining what constitutes a "concrete

---

harm that the plaintiff would have otherwise faced, absent the defendant's actions."); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (analogizing the plaintiffs' increased risk of a data breach to claims of potential future harm advanced in toxic tort cases where a plaintiff may establish standing as long as the plaintiff faced "a credible threat of harm"); Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("[T]he proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm . . . as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes.").

143. Strubel v. Comenity Bank, 842 F.3d 181, 190 (2d Cir. 2016).

144. *Id.*

145. *See* Plave & Edson, *supra* note 140, at 495–99.

146. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–02, 409–10, 414 (2013); *see*, *e.g.*, Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1284 (M.D. Fla. 2016) (finding that the alleged harm following a data breach did not meet this standard).

147. *Attias*, 865 F.3d at 628–29 (citing Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015)) ("Here . . . an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill. As the Seventh Circuit asked, in another data breach case where the court found standing, 'Why else would hackers break into a … database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.'").

and particularized harm" under Article III when an entity fails to fulfill its obligations to safeguard sensitive data. [148] Instead, it has merely kicked the can down the road. There is no end in sight for the split in federal courts regarding how to treat violations of traditional data privacy regulations or lawsuits involving traditional data breaches. By extension, it is difficult to anticipate how courts will react when the underlying data consists of biometrics rather than more innocuous information. Simultaneously, it is unreasonable to expect Congress to spend time passing legislation protecting an individual's right to their biometric data when their constituents may not ultimately be able to sue to enforce that right.

D. *Private Right of Action for Statutory Violation in a Data Privacy Context*

To be sure, it would be unnecessarily burdensome on businesses to hold them liable for damages every time, for example, a receipt was printed with a customer's full credit card expiration date,[149] or held on to some business records containing personally identifiable information after a customer had cancelled a subscription.[150] However, it is important that the law recognizes a distinction between these traditional data points and biometrics. There is a vast difference between holding on to traditional PII for an extended period as in *Braitberg* versus Facebook holding on to someone's facial signature indefinitely.[151] The last few digits of my credit card are largely useless in and of themselves. However, if bad actors possessed my face or fingerprints, this is much more cause for alarm.[152]

Today, as a result of *Spokeo*, whether intentional or not, "the enforcement of data privacy laws falls exclusively to the states, with federal courts being "mere observers in based on constitutional standing principles."[153] Meanwhile, lower federal courts have been quick to apply

148. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).

149. *See* Crupar-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76, 77 (2d Cir. 2017); Meyers v. Nicolet Rest. of de Pere, LLC, 843 F.3d 724, 725 (7th Cir. 2016). *But see* Flaum v. Dr.'s Assocs., Inc., 204 F. Supp. 3d 1337, 1339 (S.D. Fla. 2016) (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546–48 (2016)). The Southern District of Florida found standing where a defendant printed a full expiration date on a receipt in violation of the Fair and Accurate Credit Transaction Act (FACTA). *Id.*

150. *See* Braitberg v. Charter Comm. Inc., 836 F.3d 925, 930 (8th Cir. 2016).

151. *Id.*

152. *See* Pandya, *supra* note 42.

153. *See* Brian Kint, *'Spokeo' Standing Analysis After 'Rosenbach v. Six Flags*,*'* LEGAL INTELLIGENCER (July 18, 2019, 2:50 PM), http://www.evergreeneditions.com/publication/?i=603239&article_id=3432532&view=articleBrowser.

the *Spokeo* standing analysis to other data privacy cases outside of the context of the Fair Credit Reporting Act.[154] Interpreted broadly to apply to all data privacy laws regulating potential uses of personal data, *Spokeo* places a far tougher burden on plaintiffs in data privacy cases by making it more difficult for a private right of action to survive a motion to dismiss in federal court.

As a result of the uncertainty surrounding a private right of action to remedy statutory harms, courts are further split on the issue of statutory violations specifically in a data privacy context.[155] For example, the Second, Seventh, Eighth, and D.C. Circuits have all denied the existence of standing for plaintiffs alleging harm based on an alleged statutory violation in data privacy cases.[156] These circuits interpret *Spokeo* to mean that even where Congress confers a procedural right to protect a concrete interest, that does not mean a court will see a "material" violation of a plaintiff's right.[157] The question the Second, Seventh, Eighth and D.C. Circuits do not address is, in the realm of data privacy, what constitutes a "material" risk?

On the other side of this circuit split, a number of federal courts have attempted to answer this question.[158] In *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, two laptops containing information on Horizon Healthcare Services, Inc.'s members were stolen from their corporate headquarters.[159] Horizon notified its members that their personal information may have been compromised and offered free credit monitoring services to anyone who may have been impacted by the

154. Kint, *supra* note 153; *see* Crupar-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76, 77 (2d Cir. 2017); Meyers v. Nicolet Rest. of de Pere, LLC, 843 F.3d 724, 725 (7th Cir. 2016); Flaum v. Dr.'s Assocs., Inc., 204 F. Supp. 3d 1337, 1341 (S.D. Fla. 2016).

155. Plave & Edson, *supra* note 140, at 499–501.

156. *See* Strubel v. Comenity Bank, 842 F.3d 181, 185, 188 (2d Cir. 2016) (holding that an alleged violation of the Truth in Lending Act was not sufficient on its own to establish standing if the plaintiff could not show further harm) (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1556 (2016)); *Crupar-Weinmann*, 861 F.3d at 77; *Meyers*, 843 F.3d at 725 (applying an approach that is effectively the same as the Second Circuit's); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 927, 930 (8th Cir. 2016) (holding that just because the plaintiff had demonstrated a violation of a statutory right they still needed to show an "actual injury" arising from the defendant's retention of his personal information) (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1556 (2016)); Hancock v. Urban Outfitters, Inc., 830 F.3d 511, 514–15 (D.C. Cir. 2016) (holding that statutory violations alone do no create the type of injury in fact necessary to establish standing and that even in claims alleging violation of statutorily conferred rights the asserted injury must impact the plaintiff in a "personal and individual way") (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1556 (2016)).

157. *Strubel*, 842 F.3d at 190.

158. *See* Plave & Edson, *supra* note 140, at 495–500 (detailing cases in which courts have held that statutory violations alone may be sufficient to establish standing).

159. *See In re* Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).

breach.[160] These members sued, arguing that Horizon had "furnish[ed]" their information in an unauthorized fashion by allowing their information to fall into the hands of thieves and by failing to adopt reasonable procedures to keep the information confidential, amounting to a statutory violation of the FCRA.[161] The Third Circuit held that in some cases a procedural violation of the FCRA is, on its own, sufficient to establish standing for the plaintiffs themselves to bring suit.[162] They went on to assert that *Spokeo* merely reaffirms Congress' power to define injuries through legislation.[163]

The U.S. District Court for the Northern District of California adopted comparable reasoning in *Matera v. Google, Inc.*[164] There, the plaintiffs sued Google, claiming that the company had violated state and federal anti-wiretapping laws when it "intercepted the [plaintiffs'] emails for the dual purposes of (1) providing advertisements targeted to the email's recipient or sender, and (2) creating user profiles to advance Google's profit interests" without the plaintiffs' knowledge or consent.[165] After granting a motion to stay pending the Supreme Court's decision in *Spokeo*,[166] Google once again reasserted following *Spokeo* that the plaintiffs lacked standing to sue because, "Plaintiff can not [*sic*] rely 'solely on the purported statutory violations *alone* as the basis for Article III standing.'"[167]

The District Court found that *Spokeo* "clearly rejects" Google's argument,[168] holding that while not every harm recognized by statute will be sufficiently concrete for standing purposes, in this case "the existence of a private right of action, the availability of statutory damages, and the creation of a substantive private right . . . support finding that . . . Congress . . . intended to 'grant[ ] persons in [Plaintiff's] position a right to judicial relief' without additional allegations of injury."[169] The Northern District of California interpreted *Spokeo* as holding that two factors may be relevant to whether the violation of statutory rights constitutes injury in fact: (1) whether the statutory

160. *See id.* at 630.
161. *See id.* at 631.
162. *See id.* at 639–41 ("[W]ith the passage of the FCRA, Congress established that the unauthorized dissemination of [plaintiffs'] 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.").
163. *See id.* at 638.
164. *See* Matera v. Google, Inc., No. 15-CV-04062-LHK, 2016 WL 5339806 (N.D. Cal. Sept. 23, 2016).
165. *Id.* at *1.
166. *Id.* at *5.
167. *Id.* at *8.
168. *Id.* at *9.
169. *Id.* at *13 (quoting Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010)).

violation bears a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts[,]" and (2) congressional judgement in establishing the statutory right, including whether the statutory right is substantive or procedural.[170]

Given the Supreme Court's recent denial of certiorari in *Facebook v. Patel*, we now seem destined to head down the same path of deep circuit splits and confusion in terms of biometrics as we see with traditional data privacy rights.[171] Given the real potential for permanent damage to people's privacy rights, we can ill afford similar standing debates in this new context of biometrics.[172] While the risks implicated when handling traditional data are not to be taken lightly, [173] they pale in comparison to the potential harms that could occur if biometric data is handled improperly or purposely abused.[174]

CONCLUSION

Today we are all trapped in an "internet of things" without ever having given our consent.[175] The facilitators of this connectivity, whether they be social media websites, search engines, apps, or even manufacturers of household appliances,[176] have taken advantage of our government's passive deference to amass as much information about us as possible. It is not clear why exactly my refrigerator needs to be able to communicate with my oven,[177] or why it is necessary for a theme park to ask for visitors' fingerprints to gain entry.[178] But as a society, we seem to be too content with modern conveniences to cause a fuss about any of it.

Questions of whether or not we have "consented" to this way of life have become irrelevant. The trouble is not only that we did not consent to this surveillance, but the sheer futility of trying to resist being surveilled. Indeed, there is no way to "opt out" of Google Earth.[179]

---

170. *Id.* at *9.

171. Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020).

172. *See* Pandya, *supra* note 42.

173. *See* Alfred Ng, *How the Equifax Hack Happened, and What Still Needs to Be Done*, CNET (Sept. 7, 2018, 4:54 AM), https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

174. *See* Pandya, *supra* note 42.

175. *See* Ferguson, *supra* note 6.

176. *See* Garling, *supra* note 11.

177. *See* Ferguson, *supra* note 8, at 585; *see also* Garling, *supra* note 11.

178. *See generally* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

179. Amazon has sold 100 million Alexa devices and employs thousands of people to listen to the utterances of every person within earshot. *See* Matney, *supra* note 11; Valinsky, *supra* note 11.

Until the Supreme Court updates its standing analysis to suit the realities of the digital era, demonstrating a "concrete" injury in many cases will remain a lofty goal even for plaintiffs who have suffered precisely the sort of harm that data privacy statutes were written to protect. As a result, creatures of the information age now represent a looming specter of clandestine threats to privacy that our legislators in Washington lack the proper tools to combat. As long as it is unclear whether a federal solution to this problem could withstand Supreme Court scrutiny, it is unreasonable to expect Congress to act.

But the law has always evolved over time to meet the changing conditions of society.[180] Unfortunately, the way our laws develop tends to be a function of who is in the best position to use the law for their benefit.[181] Those people tend to be powerful entities with not only the resources to litigate in the first place, but also access to major instruments of private power, including that of the press, public relations agencies, lobbyists, law firms and marketing professionals.[182] Through these means, powerful entities tend to take an active role in shaping the law to benefit their already advantageous positions.[183]

Against this enemy, the best defense is a good offense. In the face of so many profoundly unscrupulous actors, the best form of government is the one that works *both* to safeguard the rights of its citizens *and* to empower its citizens to defend themselves. In response to a threat as dynamic as informational privacy in the modern era, an equally dynamic solution is required.

To this end, contrary to Justice Thomas' concurrence in *Spokeo*, legal mechanisms do exist for allowing private plaintiffs to sue bad actors who breach duties they owe to the public at-large. Specifically, the private right of action. Unleashing plaintiffs through a private right of action may be the only way for Washington D.C. to counterbalance the aggressive tactics of Silicon Valley.[184] The aptly-named "surveillance capitalists" have proven to be remarkably adept at avoiding questions about the ethical consequences of their actions to continue absorbing data unimpeded. Having reached the point where the data they consume is not just *about us*, but literally *us*, it is time to recognize an interest in biometric privacy and authorize private citizens to protect that interest

180. Aditya Shastri, *Our Society Keeps Changing. Does the Law Change Too?*, MEDIUM (May 20, 2019), https://medium.com/@adityashastri/our-society-keeps-changing-does-the-law-change-too-e12f4071d4.

181. *See* Nader, *supra* note 4, at 655–56.

182. *Id.*

183. *See id.*

184. *See id.* ("[T]he life and death of the law derive from the plaintiff, and . . . this fact is nowhere more important . . . than in our democratic society.").

by imposing statutorily-defined penalties on firms that record or transfer our biometrics without our consent through a private right of action.