GETTING INTO COURT WHEN THE DATA HAS GOTTEN OUT: A TWO-PART FRAMEWORK

INTRODUCTION

In the late summer of 2017, headlines announcing that the personal information of nearly 150 million American consumers had been compromised shocked the conscience of the nation. Equifax, a credit reporting agency that compiled the personal financial information of consumers and sold it to businesses, had been hacked.[1] During the seventy-six days in which the hack went unnoticed by Equifax, hackers surreptitiously made 9,000 search queries,[2] obtaining massive amounts of personal information including millions of consumers' names, addresses, birth dates, social security numbers, driver's license numbers, and even credit card numbers.[3] This stolen information, ranging from bank accounts to medical records,[4] is the key to much of consumers' financial lives. With it, the thieves could destroy consumers' credit worthiness and effectively impersonate individuals with creditors, employers, and service providers.[5]

Following the breach, a class of ninety-six consumers whose data had been exposed filed a complaint against Equifax in federal district court alleging "present, immediate, imminent, and continuing increased risk of harm" as a result of the breach.[6] The plaintiffs claimed they were harmed by the burden of taking additional measures to combat identity theft and the increased possibility that their identity would be stolen in the future.[7] Plaintiffs alleged damages in the form of wasted time, effort, and money spent monitoring their credit and identity, and by the "serious and imminent risk of fraud and identity theft" due to the breach.[8] The plaintiffs brought suit

1. *See* Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth & Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [https://perma.cc/5YBC-7392].

2. Glenn Fleishman, *Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says*, FORTUNE (Sept. 7, 2018, 7:12 PM), https://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/ [https://perma.cc/XH5Y-7T3B].

3. Fleishman, *supra* note 2.

4. Bernard et al., *supra* note 1.

5. *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1309 (N.D. Ga. 2019) (describing consumer reports as "linchpins" of the nation's financial system because of their central role in creditors' decisions to extend credit). *But see id.* at 1314 (holding that "[t]he Plaintiffs' argument that the information stolen in the Data Breach could bear on their credit worthiness is not persuasive").

6. *Id.* at 1309.

7. *Id.* at 1311.

8. *Id.*

under the Fair Credit Reporting Act ("FCRA"), arguing that Equifax unlawfully "furnished" their consumer reports to hackers and "failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers."[9]

The court, finding that the plaintiffs failed to state a claim under the FCRA, granted Equifax's motion to dismiss.[10] The court reasoned that, although the FCRA does not define "furnish," courts have held that information stolen by hackers is not "furnished" within the meaning of the FCRA.[11] The plaintiffs, acknowledging this precedent, argued that Equifax should still be subject to liability because its "conduct was 'so egregious' that it should be considered akin to furnishing."[12] The court disregarded this argument, stating that the plaintiffs failed to provide discernable standards by which to determine when conduct was so egregious as to be considered furnishing.[13] The court then accepted Equifax's argument that the stolen information did not relate to consumers' credit worthiness and therefore did not constitute a "consumer report" protected by the FCRA.[14] Finally, the court held that because the failure to maintain reasonable procedures claim required Equifax to have illegally released a consumer report, that claim must necessarily be dismissed upon a finding that no consumer report had been compromised.[15]

In the end, Equifax did face some consequences for its negligence. Though consumer attempts to hold Equifax accountable were unsuccessful, the Federal Trade Commission ("FTC"), along with forty-eight states, the District of Columbia and Puerto Rico, and the Consumer Financial

9. *Id.* at 1312.

10. *Id.* It is necessary to note that the court did not dismiss the FCRA claim for lack of standing. Instead, it dismissed under FED. R. CIV. P. 12(b)(6), because plaintiffs failed to state a "'plausible' claim for relief" under the FCRA. *Id.* at 1311–14.

11. *Id.* at 1312–13 ("[C]ourts generally use the term [furnish] to describe the active transmission of information to a third-party rather than a failure to safeguard the data." (quoting *In re* Experian Data Breach Litig., No. SACV 15-1592 AG (DFMx), 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016))).

12. *Id.* at 1313.

13. *Id.*

14. *Id.* at 1313–14. The FCRA defines "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or modeof living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—(A) credit . . . ; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." *Id.* at 1313 (quoting 15 U.S.C. § 1681a(d)(1)). That a consumer's private financial information—such as social security numbers, credit card information, date of birth, etc.—does not bear on that individual's "creditworthiness" is hard to believe. A credit report is nothing more than the sum of the information it contains.

15. *Id.* at 1314.

Protection Bureau ("CFPB") brought suit against Equifax to enforce provisions of the Federal Trade Commission Act ("FTC Act") and other federal consumer protection laws.[16] In July of 2019, Equifax and the FTC reached a settlement of nearly $700 million, whereby Equifax agreed to create a fund of up to $425 million to provide free credit monitoring services and restitution for out-of-pocket losses resulting from the breach.[17] In addition, Equifax agreed to pay $175 million in civil penalties to the states and a fine of $100 million to the CFPB.[18]

Though $700 million seems significant, it is not enough to remedy the severe and varying harms caused by the breach.[19] Nearly 150 million American consumers suffered substantial injuries including time and money spent securing personal accounts and consumer reports from future identity theft, costs of obtaining additional credit monitoring products or security freezes, and a vastly increased risk of falling victim to identity theft in the future.[20] Significantly, given the nature of the information stolen, data thieves could wait years before utilizing the stolen data,[21] causing protracted anxiety to millions of American consumers.

It is hard to swallow that Equifax faced only limited liability for such colossal negligence.

---

16. Complaint for Permanent Injunction & Other Relief at 2, FTC v. Equifax, Inc., No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) [hereinafter Complaint]; *see CFPB, FTC and States Announce Settlement with Equifax over 2017 Data Breach*, CONSUMER FIN. PROT. BUREAU (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/ [https://perma.cc/8N7B-CYTG]. The Complaint alleged violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which "prohibits unfair or deceptive acts or practices in or affecting commerce," and the Safeguards Rule, 16 C.F.R. § 314, which "requires financial institutions to protect the security, confidentiality, and integrity of consumer information." Complaint, *supra*, at 2.

17. Megan Leonhardt, *Equifax to Pay $700 Million for Massive Data Breach. Here's What You Need to Know About Getting a Cut*, CNBC: MAKE IT (July 22, 2019, 9:07 PM), https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html [https://perma.cc/JCP2-CNS7]. Although consumers can theoretically recover up to $20,000 for out-of-pocket losses resulting from fraud or misuse of personal information, this will be nearly impossible to establish. In order to recover for out-of-pocket losses, the consumer must prove a direct connection between "real financial loss" and the stolen data. Kate Fazzini, *Proving You Deserve $20,000 from the Equifax Settlement Will be Nearly Impossible*, CNBC (July 22, 2019, 3:38 PM), https://www.cnbc.com/2019/07/22/equifax-reveals-details-of-671-million-settlement.html [https://perma.cc/UJB7-UF8F]. However, there is currently no sign of the data the hackers took. Kate Fazzini, *The Great Equifax Mystery: 17 Months Later, the Stolen Data Has Never Been Found, and Experts Are Starting to Suspect a Spy Scheme*, CNBC (Feb. 13, 2019, 7:01 PM), https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html [https://perma.cc/2P7Z-8N4Z]. It has not appeared for sale online, and according to experts in the field, the stolen data has not been used for identity theft, fraud, or any other purpose to which stolen data is typically put. *Id.* In fact, many data breach experts think the data is likely being put to a far more nefarious purpose—the identification and recruitment of American spies by foreign governments. *Id.*

18. Leonhardt, *supra* note 17.

19. *See supra* note 17.

20. Complaint, *supra* note 16, at 14.

21. *Id.*

Because consumer reporting agencies ("CRAs") such as Equifax are oriented to serve businesses and financial institutions, instead of the average person whose data they compile, they lack effective incentives to treat ordinary consumers, and their data, well.[22] The FCRA purports to ensure the accuracy and privacy of information in the hands of CRAs,[23] but it is clear from the litigation surrounding the Equifax breach and the inability of consumers to recover under the Act that the FCRA is no longer enough protection from the risks posed by online threats to poorly protected financial information.[24]

Consumers' right to sue under the FCRA is limited, and often times private litigants struggle to state a cognizable claim within the confines of the Act.[25] Therefore, consumers do not have a truly effective avenue for recourse under federal law after their data has been compromised by a CRA. Congress should amend the FCRA to grant an explicit right of action to consumers seeking to vindicate data breach harms. However, such a private right contemplates complex problems of standing that must be resolved before such a private right can actually be meaningful. This Note will address the standing problems that would arise and propose two potential solutions.

Part I of this Note will examine the history of the FCRA, the basics of Article III standing, and its applications to intangible harms and data-privacy related injuries. Part II of this Note will then propose two potential solutions to the standing issues that arise when consumers are granted a right to sue CRAs for data breach harms. First, this Note will argue that, as the law currently stands, the Supreme Court should recognize that data breaches cause particularized and concrete harms sufficient to satisfy the injury-in-fact requirement of Article III. Finally, this Note will argue that because of judicial inconsistencies in applying the standing doctrine, state

22. *See* Consumers Union, *Don't Let Equifax Put Americans at Risk Again*, CONSUMER REPS. (Sept. 7, 2018), https://www.consumerreports.org/data-theft/dont-let-equifax-crisis-go-to-waste-equifax-data-breach/ [https://perma.cc/HYH8-DYLB].

23. FED. TRADE COMM'N, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT 1, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf [https://perma.cc/3SEJ-AQGM].

24. Equifax is not the only company that has failed to adequately protected consumer financial information from breach. *See, e.g.*, CNNMoney Staff, *Target: 40 Million Credit Cards Compromised*, CNN: BUSINESS (Dec. 19, 2013, 4:41 PM), https://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html [https://perma.cc/5KH5-BZXL]; Seena Gressin, *The Marriott Data Breach*, FED. TRADE COMM'N: BLOG (Dec. 4, 2018), https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach [https://perma.cc/CQ2P-VVYH]; Selena Larson, *Every Single Yahoo Account Was Hacked – 3 Billion in All*, CNN: BUSINESS (Oct. 4, 2017, 6:36 AM), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html [https://perma.cc/F6A5-597H]; Andrea Peterson, *Adult FriendFinder Hit with One of the Biggest Data Breaches Ever, Report Says*, WASH. POST (Nov. 14, 2016, 1:30 PM), https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/ [https://perma.cc/G3HT-BPT3].

25. *See, e.g.*, *supra* notes 10–16 and accompanying text.

legislatures should adopt a uniform law, allowing Article III standing issues to be avoided altogether.

I. THE STATUTORY AND COMMON LAW FRAMEWORK

A. The History of the FCRA

Congress enacted the FCRA to ensure that CRAs are fair, impartial, and respectful of consumers' rights to privacy.[26] The FCRA imposes a variety of responsibilities and compliance procedures on CRAs for the purpose of protecting consumers' financial information from inaccuracies, exposure, and identity theft.[27] Specifically, the FCRA requires CRAs to maintain "reasonable procedures" to ensure that they do not provide consumer reports to any person if there are "reasonable grounds" for believing that the report will not be used for a lawful purpose.[28] The FCRA, in providing a uniform standard of liability, serves to protect CRAs as well as consumers by insulating CRAs from unpredictable liability and establishing a set of clear guidelines to which they can conform their behavior.[29]

The FCRA intended to incentivize CRAs to incur the necessary costs of ensuring that consumers' data is kept private and reported accurately.[30] However noble the FCRA's prerogative, it lacks sufficient bite and enforcement power to ensure that the rights of those whom it strives to protect are in fact protected.[31] Federal and state agencies entrusted with enforcement power[32] often lack the resources[33] to pursue all violations of the FRCA, and usually do not have sufficient familiarity of the facts underlying a claim to adequately represent consumers who have been

26. 15 U.S.C. § 1681(b).

27. *See, e.g.*, 15 U.S.C. §§ 1681c-1 to -2 (requiring CRAs to take measures to insulate consumers from the effects of fraud and identity theft, such as blocking the reporting of credit information in a consumer's file that was the result of fraud or theft); 15 U.S.C. § 1681e (requiring CRAs wishing to access consumer reports to identify themselves, state the purposes for which the reports will be used, and verify that the reports will not be used for any other purpose).

28. 15 U.S.C. § 1681e; *see also supra* notes 6–11 and accompanying text.

29. Brief of Amici Curiae Information Privacy Law Scholars in Support of Respondent at 3–17, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) [hereinafter Spokeo Brief].

30. *See id.* at 5–6.

31. *See* Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism that Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html [https://perma.cc/MP78-ZGPQ].

32. Federal agencies with this power include the Federal Trade Commission and the Consumer Financial Protection Bureau. Meir Feder & Rajeev Muttreja, *Understanding the Fair Credit Reporting Act*, PRACTICAL L.J., Apr./May 2016, at 48, 50.

33. *See* Robbie McBeath, *Can the FTC Protect Consumers in the Digital Age?*, BENTON (Nov. 30, 2018), https://www.benton.org/blog/can-ftc-protect-consumers-digital-age [https://perma.cc/58DP-357L].

harmed when they do decide to act.[34] Thus, the responsibility to ensure that the act is enforced falls on the shoulders of the consumers themselves.[35] As seen in the consumer litigation arising from the Equifax breach,[36] the FCRA is insufficient to vindicate consumer privacy.[37] An express private right of action will strengthen consumer protection, promote compliance with the FCRA, and incentivize CRAs to ensure that consumer data is well protected and not at risk of theft or fraud.[38] However, even if such a right were to exist, consumers would have to overcome the substantial hurdle imposed by Article III's "injury-in-fact" requirement.[39]

B. Article III Standing and the Challenges of Data Breach Harms

The United States federal government is one of limited and divided powers.[40] Central to that principle is the requirement that the federal judicial power extends only to "Cases" and "Controversies,"[41] justiciable within the limits of the United States Constitution.[42] The doctrine of standing is closely related to the "case" or "controversy" requirement and serves to separate cases that are properly before the federal courts and those that are not.[43] The standing doctrine limits the scope of the federal judicial power by restricting the types of litigants that are "empowered" to bring suit in federal court.[44] The "irreducible constitutional minimum of standing" requires (1) an injury-in-fact, (2) causally connected to the conduct

34. *See* Jessica Rich, Opinion, *Give the F.T.C. Some Teeth to Guard Our Privacy*, N.Y. TIMES (Aug. 19, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html [https://perma.cc/48KN-GX23].

35. *See* Rich, *supra* note 34.

36. *See supra* notes 5–15 and accompanying text.

37. *See supra* notes 11–14 and accompanying text.

38. *See infra* Part II.

39. *See infra* Part II.A.

40. *See* U.S. CONST. art. I–III; *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 559–60 (1992) ("[T]he Constitution's central mechanism of separation of powers depends largely upon common understanding of what activities are appropriate to legislatures, to executives, and to courts.").

41. U.S. CONST. art. III, § 2.

42. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) ("[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal- court jurisdiction to actual cases or controversies." (alteration in original) (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997))).

43. *See Lujan*, 504 U.S. at 560 (explaining the doctrine of standing sets "apart the 'Cases' and 'Controversies' that are of the justiciable sort referred to in Article III," and "identif[ies] those disputes which are appropriately resolved through the judicial process."); *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.").

44. *Spokeo*, 136 S. Ct. at 1547.

complained of, that is (3) likely to be redressed by a favorable decision of the court.[45]

1. Standing and Intangible Harms

The Supreme Court's application of standing principles to intangible harms is complex, multifaceted, and often contradictory.[46] Both before and after the seminal privacy case *Spokeo, Inc. v. Robins*,[47] the Court has been skeptical of plaintiffs alleging intangible injuries such as stigmatic, privacy, and speculative chain[48] harms. Supreme Court precedent in these areas is a useful tool for examining the theories and processes by which the Court segregates the harms it deems legally cognizable within Article III from those it does not.

For example, in *FEC v. Akins*,[49] the Court held that an alleged infringement of a statutory right was alone sufficient to satisfy Article III injury-in-fact. In *Akins*, plaintiff-voters brought suit challenging a decision of the Federal Election Commission ("FEC") that the American Israel Public Affairs Committee ("AIPAC") was not a "political committee" and therefore was not required to make the disclosures required of organizations so designated.[50] The FEC Act[51] authorized suit by any person "aggrieved" by an FEC decision. The plaintiffs alleged that these disclosures would help them better evaluate candidates for public office, and that the deprivation of this information was a legally cognizable injury.[52] The Court allowed standing.[53] It reasoned that, through the enactment of the FEC Act, Congress statutorily created a right to information about political committees, and that plaintiffs were denied that information because of the FEC's decision.[54] In essence, the Court found an alleged infringement of the statutory right established by the FEC Act sufficient to meet Article III's injury-in-fact requirement.[55]

---

45. *E.g.*, *Lujan*, 504 U.S. at 560–61; Whitmore *ex rel.* Simmons v. Arkansas, 495 U.S. 149, 155 (1990); Simon v. E. Ky. Welfare Rts. Org., 426 U.S. 26, 41–42 (1976).

46. *See infra* notes 49–80 and accompanying text.

47. 136 S. Ct. 1540; *see infra* Part I.B.2.

48. *See infra* notes 64–75 and accompanying text.

49. 524 U.S. 11 (1998).

50. *Akins*, 524 U.S. at 15–16.

51. The FEC Act constitutes the bulk of U.S. campaign finance law. It places limits on campaign contributions to federal candidates and political parties and creates requirements for the disclosure of public financing. *Federal Law*, CAMPAIGN FIN. INST., http://www.cfinst.org/law/federal.aspx [https://perma.cc/5JWY-AC5J].

52. *Akins*, 524 U.S. at 16–17.

53. *Id.* at 19.

54. *Id.* at 20.

55. *Id. Compare id.* (finding a statutory violation to be sufficient for Article III standing), *with* Spokeo v. Robins, 136 S. Ct. 1540 (2016) (finding that a bare statutory violation is not sufficient for Article III standing absent an injury-in-fact).

The Court has thus far been reluctant to find stigma or anxiety alone to be a harm sufficient to establish Article III standing. In *Allen v. Wright*,[56] the plaintiffs, parents of Black public-school children during the desegregation era, sued the Internal Revenue Service ("IRS") challenging the agency's failure to deny tax-exempt status to racially discriminatory private schools.[57] The plaintiffs claimed that they were harmed by the stigmatizing effect of racial discrimination as promoted by the IRS.[58] The Court, though sympathetic, firmly held that "abstract stigmatic injury" alone is not cognizable under Article III.[59] Similarly, in the recent case of *Trump v. Hawaii*,[60] the Court declined to consider whether stigma was sufficient to confer Article III standing. In *Trump*, the plaintiffs, United States citizens and permanent residents, challenged President Donald Trump's proclamation that restricted entry into the United States by nationals of six majority Muslim countries.[61] The plaintiffs argued that they had suffered a "claimed dignitary interest" in being free from federal religious establishments and the designation of a "disfavored faith".[62] The Court declined to decide whether this dignitary interest was adequate for Article III standing.[63]

The Court has also declined to confer standing where the plaintiff could prove no more than a speculative chain of possibilities.[64] In *Clapper v. Amnesty International USA*,[65] a group of lawyers and human rights groups brought suit claiming injury under the Foreign Intelligence Surveillance Act ("FISA").[66] They alleged that, because they communicated with clients in areas that were heavily monitored as part of counterterrorism efforts, there was an "objectively reasonable likelihood" that their communications would

56. 468 U.S. 737 (1984).

57. *Id.* at 743.

58. *Id.* at 754.

59. *Id.* at 755–56. Although the Court ultimately holds that stigma is not sufficient for Article III standing, it does acknowledge the very real harm that stigma causes. The Court states: "There can be no doubt that this sort of noneconomic injury is one of the most serious consequences of discriminatory government action" and even goes so far as to state that in some circumstances, stigmatic injuries may be sufficient to support Article III standing. *Id.* at 755. However, the Court specifies that stigmatic injury "accords a basis for standing only to 'those persons who are personally denied equal treatment' by the challenged discriminatory conduct." *Id.* (quoting Heckler v. Mathews, 465 U.S. 728, 739–40 (1984)).

60. 138 S. Ct. 2392 (2018).

61. *Id.* at 2406.

62. *Id.* at 2416.

63. *Id.* The Court granted standing on other grounds, finding that the plaintiffs "assert[ed] another, more concrete injury: the alleged real-world effect that the Proclamation has had in keeping them separated from certain relatives who seek to enter the country." *Id.*

64. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410–11 (2013).

65. *Id.*

66. For general information on FISA, see *Foreign Intelligence Surveillance Act (FISA)*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/surveillance/fisa/ [https://perma.cc/WB39-55CM].

be intercepted.[67] Fear of being monitored caused the plaintiffs to take costly measures to protect confidentiality, including frequently flying overseas to meet with clients instead of communicating over telephone or other electronic means.[68] The Court found that the plaintiffs lacked standing because they could not show with reasonable certainty that their conversations were actually being surveilled.[69] The Court stated that plaintiffs' claim rested on a speculative chain of possibilities, and that they could not show that an injury based on potential future surveillance was "certainly impending"[70] in order to establish Article III standing. Significantly, the Court did not accept the plaintiffs' argument that the money spent to preserve confidentiality constituted a cognizable injury under Article III.[71] The Court held that one cannot "manufacture" standing based on fears of "hypothetical future harm."[72]

However, the Court's "speculative chain of possibilities" reasoning in *Clapper* is inconsistent with other recent Supreme Court opinions. In *Massachusetts v. EPA*[73] and *Department of Commerce v. New York*,[74] the Court has found similarly abstract and speculative chains of reasoning sufficient to support standing. In *Massachusetts*, the State of Massachusetts claimed an injury resulting from the EPA's refusal to promulgate greenhouse emissions standards.[75] Massachusetts alleged that, as a result of the EPA's failure to regulate, it was likely to lose valuable costal property due to global warming traceable to greenhouse gas emissions from cars and a consequential rise in sea levels.[76] Though Massachusetts' injury seems to be significantly more abstract than that alleged by the plaintiffs in *Clapper*, the Court found Article III standing to be satisfied.[77] Likewise, in *Department of Commerce*, the Court again found a chain of possibilities to be the basis for standing in ruling that plaintiff-states could challenge the inclusion of a citizenship question on the 2020 census questionnaire.[78] In *Department of Commerce*, the plaintiff states claimed that the "citizenship

67. *Clapper*, 568 U.S. at 401.
68. *Id.* at 401–02.
69. *Id.*
70. *Id.*
71. *Id.* at 402.
72. *Id.*
73. 549 U.S. 497 (2007).
74. 139 S. Ct. 2551 (2019).
75. *Massachusetts*, 549 U.S. at 521–23.
76. *Id.* According to Massachusetts' affidavits, global sea levels have risen between ten and twenty centimeters over the 20th century because of global warming. *Id.* at 522.
77. *Id.* at 526. This injury seems highly conjectural, abstract, and attenuated. It seems quite unlikely that new emissions standards would actually slow global warming enough to prevent the loss of coastal property. However, the Court has historically given more leeway to states as plaintiffs on standing issues. *Id.* at 518–19.
78. *Department of Commerce*, 139 S. Ct. at 2565.

question would result in noncitizen households responding to the census at lower rates than other groups, which in turn would cause them to be undercounted" and lead to loss of federal funds.[79] The Court distinguished *Clapper*, finding that the plaintiffs theory of standing "[did] not rest on mere speculation" and that it "relies instead on the predictable effect of Government action on the decisions of third parties."[80]

2. Spokeo v. Robins *and the Evolution of "Injury"*

Because data breach harms are often speculative or intangible,[81] the injury-in-fact requirement is a significant hurdle to plaintiffs wishing to vindicate their rights in federal court for data breach harms.[82] In *Spokeo, Inc. v. Robins*[83] the Supreme Court attempted to clarify the Article III standing requirements for data-privacy related cases. In *Spokeo*, the plaintiff, Robins, brought an FCRA action in federal court against Spokeo, Inc. ("Spokeo") a self-proclaimed "people search engine," for inaccurate reporting of his personal information.[84] Robins alleged that his Spokeo profile inaccurately stated that he was married, had children, was in his fifties, had a job and a graduate degree, and was relatively wealthy.[85] Robins claimed that these misrepresentations harmed his employment prospects because the profile made him seem overqualified for jobs he may have otherwise been offered, "expectant of a higher salary than employers would be willing to pay," and "less mobile because of family responsibilities."[86]

The district court found that Robins lacked standing and dismissed his complaint, but the Ninth Circuit reversed on appeal, finding that he had alleged sufficient injury-in-fact to satisfy Article III.[87] The Supreme Court

79. *Id.*

80. *Id.* at 2566.

81. Examples of harms that might arise from data breaches include the risk of pecuniary loss resulting from potential fraud/identity theft, preventative measures to protect against risk of future pecuniary loss, invasion of privacy, and anxiety and emotional distress. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018); Elizabeth C. Pritzker, *Making the Intangible Concrete: Litigating Intangible Privacy Harms in a Post*-Spokeo *World*, 26 COMPETITION 1 (2017); *see also supra* note 17 and accompanying text.

82. *See infra* Part II.A.

83. 136 S. Ct. 1540 (2016).

84. *Id.* at 1544. Spokeo is a searchable, yellow-pages-like website that allows curious individuals to input a person's name, phone number, or email address and view a report of their personal information compiled from a variety of databases. *Id.* Upon running a search for my own name, Spokeo provided me with a wealth of information about myself—my address, my parents' addresses, my approximate income, my level of education, and my general consumer tendencies.

85. *Id.* at 1546.

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

87. *Id.* at 1544 (majority opinion). The Ninth Circuit reasoned that Robins had alleged a violation of his own statutory rights and that he had an individualized, rather than collective, interest in his own credit and personal information. *Id.*

of the United States reversed, finding that the Ninth Circuit had misapplied the standing doctrine, and outlined what was to become the current state of the injury-in-fact requirement in data-privacy scenarios.[88]

The Court emphasized the importance of injury-in-fact to the standing doctrine and the larger policy of separation of powers.[89] Specifically, the Court made clear that injury-in-fact is an "irreducible constitutional minimum" that cannot be erased or legislated away by a congressional grant of a right to sue, given through statute, to a plaintiff who would otherwise not satisfy the requirements to get into federal court.[90] The Court then articulated that injury-in-fact requires an "invasion of a legally protected interest" that is both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[91] The Court states that a particularized harm is one that affects the plaintiff in a "personal and individual way."[92] Elaborating, the Court states that a harm must be not only particularized, but concrete, and that concreteness is a requirement distinct from particularization.[93] The Court states that a concrete injury is one that "actually exist[s]," and is real, rather than abstract.[94] However, the Court specifies that concrete injuries need not be tangible in the traditional sense. In fact, the Court outlines two factors to consider when determining whether an intangible harm constitutes an "injury-in-fact": 1) whether the alleged intangible harm has 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) whether Congress intended the harm to meet Article III requirements.[95] The Court acknowledges that Congress has the power to elevate by statute "legally cognizable injuries" that were not previously recognized at law.[96] But these harms must still meet the minimum requirements mandated by Article III, and Congress cannot legislate standing where it would otherwise not exist.[97] In other words, bare statutory

88. *See id*. at 1545.
89. *Id.* at 1546–50; *see supra* notes 40–43 and accompanying text.
90. *Spokeo*, 136 S. Ct. at 1547–48.
91. *Id.* at 1548 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).
92. *Id.* (quoting *Lujan*, 504 U.S. at 560 n.1).
93. *Id.* According to the Court, it is here that the Ninth's Circuit's analysis went astray. The Court finds that the Ninth Circuit "elided" the concreteness with particularization, stating that Robins' injury was sufficiently concrete when it was in fact only particularized. *Id.*
94. *Id.* The Court also notes that Congress is not restricted from, by statute, "elevat[ing] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Id.* at 1549 (quoting *Lujan*, 504 U.S. at 578). But these intangible harms must still satisfy the minimum requirements of Article III. *Id.*
95. *Id.* at 1549.
96. *Id.*; *see supra* note 94.
97. *Spokeo*, 136 S. Ct. at 1548; *supra* note 94.

violations, without a concrete and particularized injury-in-fact, do not confer standing.[98]

The Court concluded that the Ninth Circuit had not fully appreciated "concreteness" as a discrete element of injury-in-fact and remanded for a determination of whether or not Robbins had alleged a sufficiently concrete and particularized injury.[99] Though the Court admits that Congress enacted the FCRA in part to minimize the dissemination of false information by adopting procedures to decrease that risk, a mere violation of those procedures does not necessarily create the type of harm that is legally cognizable under Article III.[100] Significantly, the Court states that a "violation of one of the FCRA's procedural requirements may result in no harm," and not all inaccuracies, like those affecting Robins, cause the type of harm that can give rise to standing in federal court.[101]

II. FACILITATING A PRIVATE RIGHT: THE SUPREME COURT OR THE STATES?

Consumer protection laws, such as the FCRA, can only be effective if victimized consumers are allowed to vindicate their own rights in court. Because private individuals largely cannot bring suit under the FCRA, injuries caused by consumer privacy violations are often left unredressed.[102] The following Part of this Note will first outline the merits of a private right of action and argue that a such a right should be expressly conferred by Congress. However, the gift or implication of a private right of action is itself a solution that raises the primary issue this Note seeks to address: standing. Given the current state of the standing doctrine as it pertains to intangible harms post-*Spokeo*,[103] it is unlikely that the federal courts would actually reach the merits of many data privacy cases even if these cases were brought by the consumers themselves. Therefore, the remainder of this Note will first argue that the Supreme Court should recognize that the harms caused by data breaches are sufficiently "particularized" and "concrete." Then, this Note will explore an alternative solution to the standing problem

98. *Spokeo*, 136 S. Ct. at 1549. It is difficult to reconcile the Court's holding in *Akins* with its holding in *Spokeo* less than twenty years later. In *Akins*, the plaintiffs were alleging an intangible harm—lack of information—that arose by virtue of a mere statutory violation. Likewise, in *Spokeo*, the plaintiff alleged a procedural violation of the FCRA. It seems nonsensical to consider the harm in *Akins* to be any more "concrete" than that alleged in *Spokeo*.

99. *Id.* at 1550.

100. *Id.*

101. *Id.* The Court provides several examples to illustrate this point: (1) "[E]ven if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate," and (2) "An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm." *Id.*

102. *See supra* notes 30–39 and accompanying text.

103. *See supra* Part I.B.2.

and argue that, given the inconsistencies of federal court standing jurisprudence, a uniform state law granting consumers a private right of action should be considered.

Enforcement of the FRCA and other federal statutes intended to promote consumer protection have largely been left to federal agencies.[104] In particular, the FTC is primarily responsible for the administration of consumer protection laws such as the FTC Act and the FCRA.[105] However, though the FTC rigorously attempts to enforce data and consumer privacy legislation, its power is not unlimited. Federal agencies often lack the resources necessary to prosecute all, or even most, violations of its rules.[106]

On the other hand, many benefits emerge when private citizens are allowed to vindicate their own rights under federal law. For example, private enforcement increases prosecutorial resources and conserves federal funds by allowing agencies to focus their enforcement efforts on violations that don't incentivize private litigants to sue.[107] Additionally, private litigants are better equipped with the information necessary to effectively vindicate the harms they personally suffered.[108] Also, private enforcement encourages legal innovation because private litigants are more likely than agency prosecutors to push for expansions in liability and the development of new legal standards that push the envelope of administrative regulatory policies.[109] Further, the decentralized nature of private litigation promotes innovation by allowing district judges to experiment with a number of various policy solutions to widespread issues.[110] In this way, courts can act as laboratories of democracy by developing common law ideals that, if effective, can grow to national prominence. Finally, consumer enforcement

104. The FTC's Bureau of Consumer Protection is the arm of the FTC that "stops unfair, deceptive and fraudulent business practices by: collecting complaints and conducting investigations, suing companies and people that break the law, developing rules to maintain a fair marketplace, [and] educating consumers and businesses about their rights and responsibilities." *About the Bureau of Consumer Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection [https://perma.cc/2S8G-ZEKJ].

105. *Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement [https://perma.cc/DVX9-HBT7].

106. Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal US Privacy Legislation*, INT'L ASS'N OF PRIV. PROS. (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/#:~:text=rss_feed-,Private%20right%20of%20action%20shouldn't%20be%20a%20yes%2Dno,in%20federal%20US%20privacy%20legislation&text=Privacy%20advocates%20recommend%20individuals%20be,without%20any%20showing%20of%20harm [https://perma.cc/G4XY-N8NS].

107. Stephen B. Burbank, Sean Farhang & Herbert M. Kritzer, *Private Enforcement,* 17 LEWIS & CLARK L. REV. 637, 662–63 (2013).

108. *Id.* "[T]he massive governmental expenditures required to detect and investigate misconduct are no match for the millions of 'eyes on the ground' that bear witness to . . . violations." *Id.* at 664 (omission in original) (quoting Myriam E. Gilles, *Reinventing Structural Reform Litigation: Deputizing Private Citizens in the Enforcement of Civil Rights*, 100 COLUM. L. REV. 1384, 1413 (2000)).

109. *Id.*

110. *Id.*

reduces the uncertainty that inevitably results when enforcement power is left entirely to administrative agencies.[111]

Though the benefits of a private right of action are clear,[112] the standing doctrine as currently applied to data breach harms effectively prevents the federal courts from reaching the merits of these cases even if such a private right were available. Therefore, the Supreme Court should reconceptualize harms faced by data breach victims as particularized and concrete, and therefore within the parameters of federal standing doctrines.

A. Court's Solution: Data Breaches Cause Particularized and Concrete Harms Sufficient to Satisfy Art. III

The standing doctrine, while fundamental to the federal court system, is imperfect. It is applied inconsistently by the Supreme Court[113] and is oftentimes used as a mechanism for avoiding the merits of contentious cases. In addition, many injuries that are not legally cognizable under the standing doctrine do in fact produce real world harms that should be recognized by the federal courts.[114] Data breach harms are one such example. As discussed above, consumers who've been victimized by data breaches often suffer very real injuries such as emotional distress, anxiety, and pecuniary losses. But because the federal courts by and large refuse to reach the merits of these claims, private plaintiffs wishing to vindicate their rights would likely be unable to successfully bring suit in federal court, even if such a right of action were to be granted by congress.[115] Therefore, the Supreme Court should recognize intangible injuries caused by data breaches to be legally cognizable, and thereby pave the road for consumers to vindicate their harms in federal court.

In the years following the *Spokeo* decision, the Supreme Court has yet to clarify how the standing test in *Spokeo* is to be satisfied.[116] Therefore, the lower courts have applied the test in a widely divergent manner. For example, in *Strubel v. Comenity Bank*,[117] the Second Circuit held that an "alleged procedural violation can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents a 'risk of real harm' to

111. *Id.* at 664–65.
112. *See e.g.*, *id.* at 662–66; Jerome, *supra* note 106.
113. *See supra* Part I.B.1.
114. *See* Solove & Citron, *supra* note 81; Pritzker, *supra* note 81; *see also supra* note 17.
115. *See* Solove & Citron, *supra* note 81; Pritzker, *supra* note 81.
116. *See* Frank v. Gaos, 139 S. Ct. 1041, 1046 (2019) (remanding to the district court for factual determination of whether or not the *Spokeo* test was satisfied without clarifying how that test was to be applied).
117. 842 F.3d 181 (2d Cir. 2016).

that concrete interest."[118] The Third Circuit similarly applied *Spokeo* in *In re Nickelodeon Consumer Privacy Litigation*,[119] finding that "injury-in-fact 'may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'"[120]

Significantly, many lower courts have found that data breaches pose a concrete and particularized risk of harm that is sufficient to satisfy Article III. For example, the court in *Boone v. T-Mobile USA Inc.*,[121] boldly asserted that "[p]rivacy violations can give rise to standing."[122] Specifically, the *Boone* court found the mere unauthorized disclosure of personal information alone to be a concrete injury within the meaning of *Spokeo* and Article III.[123] To do so, the court in *Boone* relied on language from the Supreme Court in *Spokeo* itself: that an intangible injury is nevertheless concrete if it "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[124] The court then analogized the harms posed by privacy violations to those created by libel and slander, noting that "victims of slander and libel have long been permitted recovery even through their harms are often difficult to prove or measure."[125] The *Boone* court then stated that "[t]he FCRA elevates this harm [posed by privacy violations] to a statutory right and establishes that 'the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm.'"[126] Further, one court has found emotional distress caused by a violation of the FCRA to be sufficient injury for federal standing.[127] In *Larson v. Trans Union, LLC*,[128] the district court relied on the Supreme Court's holding in *FEC v. Akins*,[129] finding that the plaintiff suffered an "informational" injury, and not a "bare procedural violation" when defendant Trans Union provided him with a credit report containing

118. *Id.* at 190 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

119. 827 F.3d 262 (3d Cir. 2016).

120. *Id.* at 273 (quoting *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 134 (3d Cir. 2015)).

121. Civ. No. 17-378-KM-MAH, 2018 WL 588927, at *6 (D.N.J. Jan. 29, 2018).

122. *Id.*

123. *Id.*

124. *Id.* at *7 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

125. *Id.* (citing *Spokeo*, 136 S. Ct. at 1549). The *Boone* court further states that "'unauthorized *disclosures* of information' have long been seen as injurious" and argues that unauthorized disclosure is significantly similar to invasion of privacy torts that have traditionally provided a cause of action in English and American tort law. *Id.* at *8 (emphasis in original) (quoting *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 638 (3d Cir. 2017)).

126. *Id.* at *8 (quoting *In re Horizon Healthcare*, 846 F.3d at 639).

127. Larson v. Trans Union, LLC, 201 F. Supp. 3d 1103 (N.D. Cal. 2016).

128. *Id.*

129. 524 U.S. 11 (1998); *see supra* notes 49–55 and accompanying text.

misleading information.[130] Significantly, the court related the emotional distress suffered by the plaintiff to the "uncertainty" surrounding the state of his credit report and personal financial information.[131] This connection—that uncertainty can cause a kind of emotional distress legally cognizable by the federal courts—is a foundational peg on which the hat of cognizable data breach harms can be hung.

The Sixth Circuit has even recognized the increased risk of identity theft as legally cognizable.[132] For example, in *Galaria v. Nationwide Mutual Insurance*[133] the plaintiff class brought suit against Nationwide Mutual Insurance for negligently allowing their personal data to be exposed by hackers.[134] Significantly, the court eschewed the limitation seemingly imposed by *Clapper v. Amnesty International USA*[135] that allegations of "possible" future injury are insufficient. In contrast, the *Galaria* court boldly found that plaintiff suffered a "substantial risk" of harm in addition to "reasonably incurred mitigation costs," and that these injuries, though indeterminate, were sufficient for Article III standing.[136] This holding, though set out in an unpublished opinion, establishes a framework for recognizing as legally cognizable the types of harms suffered by data breach victims.

It is not enough that several remote courts have allowed standing for data breach harms. Every consumer across the nation whose data has been exposed deserves the comfort of knowing that there is a federal court in which their claims can be brought, and the assurance of knowing that the merits of their cases will be heard. The Supreme Court should, when given the chance, build on the holdings of these few and brave lower courts to hold that anxiety, emotional distress, and the pecuniary losses incurred through "mitigation costs" are sufficiently concrete and particularized to give rise to federal standing.

B. Legislatures' Solution: The United States Should Adopt a Uniform State Law Mirroring the CCPA.

The above proposal contemplates the role of the federal courts in creating an avenue by which data breach victims can uphold their rights. However, given the observed inconsistencies in the federal courts' application of standing doctrine, the federal courts are an inadequate safeguard for

130. *Larson*, 201 F. Supp. 3d at 1106.
131. *Id.* at 1108.
132. Galaria v. Nationwide Mut. Ins., 663 F. App'x 384 (6th Cir. 2016).
133. *Id.*
134. *Id.* at 385.
135. 568 U.S. 398 (2013); *see supra* notes 64–74 and accompanying text.
136. *Galaria*, 663 F. App'x at 388.

individual rights in the data breach context. Because state courts are not bound by Article III, the state legislatures should adopt a uniform state law authorizing a private right of action for data breach harms.

Since 1892, states have elected to adopt uniform state laws on issues of national importance.[137] These laws are intended to "minimize conflicts of law" between the states and offer alternatives to the "nationalization of law . . . by the [federal] government."[138] Uniform state laws are proposedby the Uniform Law Commission ("ULC"),[139] an organization created by the American Bar Association ("ABA"), for the purpose of determining which areas of the law are ripe for unification, and drafting and proposing legislation in those areas.[140] Because of the increasingly interdependent nature of the national economy, uniform state laws are becoming necessary to facilitate national commercial policies, promote economic and social development, and provide certainty among the states.[141] For example, variability in state commercial law would create an administrative nightmare for large corporations,[142] and could potentially hinder nationwide economic growth.[143]

137. *See* Robert Stein, *Strengthening Federalism: The Uniform State Law Movement in the United States*, 99 MINN. L. REV. 2253, 2255–57; Kim Quaile Hill & Patricia A. Hurley, *Uniform State Law Adoptions in the American States: An Explanatory Analysis*, PUBLIUS, Winter 1988, at 117, 117.

138. Hill & Hurley, *supra* note 140, at 117. The "states' rights" rational for adoption of uniform laws is interesting: "[A] state which unites with other states in framing such general and uniform laws in matters affecting the common interests of all the states, and in the spirit of mutual compromise, through mutual commissions and investigations, yields, in so doing, nothing whatever of its state sovereignty. On the contrary, the proposed method of voluntary state action takes from the general government any excuse for absorbing powers now confined to the states, and therefore directly tends to preserve intact the independence of the states." *Id.* at 119 (alteration in original) (quoting Paul L. Wilbert, *Uniform State Law: An Instrument for Preserving State Integrity and Sovereignty*, 49 J. KAN. BAR ASS'N 341, 346 (1980)).

139. Prior to 2008, the ULC was known as the National Conference of Commissioners on Uniform State Laws. Richard B. Long, *Uniform State Laws: Where Do They Come from and Why Do They Matter?*, N.Y. ST. BAR ASS'N J., Apr. 2019, at 32, 33.

140. Hill & Hurley, *supra* note 140, at 117–19. Since its inception in 1892, the ULC has drafted more than 250 uniform laws. Stein, *supra* note 140.

141. *See* Stein, *supra* note 140, at 2264–65, 2271.

142. *Id.*; *Joshua* Gutter & Carlton Fields, *The Imitation Game: How the CCPA Is Inspiring Other States to Regulate Consumer Data and Online Privacy*, JD SUPRA (Sept. 12, 2019), https://www.jdsupra.com/legalnews/the-imitation-game-how-the-ccpa-is-81376/ [https://perma.cc/ST6P-DV3X]. Gutter and Fields emphasize the necessity of uniformity in data privacy laws and liability as more states adopt nuanced consumer data and online privacy laws. *Id.*

143. *See* Hill & Hurley, *supra* note 140, at 118–19; *see also* Stein, *supra* note 140, at 2253 ("In order for state law to be a viable alternative to federal law on issues as to which uniformity is desirable, it is essential that state law be uniform from state to state.").

1. State Standing Principles

Given that Article III poses a stringent limitation on bringing data privacy cases in the federal courts,[144] this problem is especially suited for uniform state legislation. State courts are not bound by the same Constitutional restrictions on jurisdiction as are the federal courts.[145] This means that states are free to formulate their own standing doctrines and have the liberty to allow cases into state court that would otherwise not be justiciable in federal court. Though states are not required to follow the limitations imposed by the Constitution, the majority of states have in fact adopted standing doctrines similar to, or derived from, the "case" or "controversy" requirement of Article III.[146] However, only a minority of those states following Article III have adopted the limitations outlined in *Lujan*,[147] and even those that do recognize such limitations allow for exceptions.[148] Therefore, though the fifty states boast widely differing standing doctrines, in general, they are less demanding than those limitations imposed by the federal Constitution.[149]

a. How States and the EU Handle Data Breach Claims

Though oftentimes the law is slow to catch up with the ever-changing advances in technology, the European Union's ("EU") enactment of the General Data Protection Regulation ("GDPR") heavily influenced the global political economy and its views on data privacy regulations.[150] While technically the GDPR only effects the EU—only EU citizens benefit from the rights conferred by the Act[151]—U.S. companies that have a web

144. *See supra* Part I.B.

145. *See, e.g.*, N.Y. State Club Ass'n, Inc. v. City of N.Y., 487 U.S. 1, 8 n.2 (1988) ("[T]he special limitations that Article III of the Constitution imposes on the jurisdiction of the federal courts are not binding on the state courts.").

146. Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE AGRIC. & NAT. RES. L. 349, 349–53 (2015).

147. *See supra* notes 43–52 and accompanying text.

148. Sassman, *supra* note 149, at 349–53. For an analysis of the extent to which each state incorporates federal standing doctrines, see *id.* at 354–98.

149. *See id.* at 349–53.

150. Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGIT. GUARDIAN: DATA INSIDER (Sept. 30, 2020), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection [https://perma.cc/HR6V-NYMK]. The GDPR went into effect on May 25, 2018. *Id.*

151. These rights are extensive. The GDPR requires that companies gain consumers' consent before collection of personal data and explain how that data is used. It gives consumers the right to ask how their data is being collected and stored and the ability to require that personal data be deleted. Arielle Pardes, *What is the GDPR and Why Should You Care?* WIRED (May 24, 2018, 6:00 AM), https://www.w

presence in the EU will be required to comply with its regulations.[152] In response to the GDPR, California enacted its own formulation of the EU's comprehensive data privacy standards and several other states followed suit.[153]

The California Consumer Privacy Act ("CCPA") went into effect on January 1, 2020.[154] The CCPA is the first state-wide, comprehensive, data-privacy act, and it reflects many of the police and regulatory imperatives of the EU's GDPR.[155] The CCPA contains extensive data privacy regulations with the purpose of accomplishing three significant data privacy goals: 1) consumers will have the right to know what information is being collected about them by corporations, 2) consumers will have the right to tell data-collecting corporations not to share and sell their personal information, and 3) consumers will be protected against businesses that do not value consumer privacy.[156] Similar to the way the GDPR affects U.S. businesses operating in the EU, the CCPA likewise applies to out-of-state, for-profit corporations that collect and control the personal information of California residents, do business in the state of California, and meet certain financial requirements.[157]

In contrast to the FCRA, which does not allow a private right of action for consumers seeking to vindicate data breach injuries,[158] the CCPA breaks new ground by facilitating consumer suits following data breach harms.[159]

---

ired.com/story/how-gdpr-affects-you/ [https://perma.cc/9J39-HAP7]. Furthermore, "personal data" is widely defined to include not only a consumer's name, email, and IP address, but also "pseudonymized information" that can be traced back to that consumer. *Id.*

152. Yaki Faitelson, *Yes, the GDPR Will Affect Your U.S.-Based Business*, FORBES (Dec. 4, 2017, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/?sh=3f1933ea6ff2 [https://perma.cc/HX6W-LULD].

153. *See infra* Figure 1: State Privacy Legislation Comparison Chart.

154. Geoffrey A. Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST: TECH. (Feb. 19, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/?arc404=true [https://perma.cc/L2LH-QTJM].

155. *See* Jessica Cowle, *What Is the California Consumer Privacy Act (CCPA)?*, LOGICWORKS (Mar. 21, 2019), https://www.logicworks.com/blog/2019/03/what-is-the-ccpa/ [https://perma.cc/DQ85-ZQ7D].

156. *See* Mark Diamond, *Quick Overview: Understanding the California Consumer Privacy Act (CCPA)*, ASS'N OF CORP. COUNS. (July 26, 2019), https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa [https://perma.cc/8BDC-TYHZ]; *About Us*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/about [https://perma.cc/74SU-RY47].

157. Diamond, *supra* note 159. An out-of-state corporation must meet one of the following three requirements before they will be required to comply with the CCPA: 1) have an annual gross revenue above $25 million, 2) receive or disclose the personal information of at least 50,000 California residents, or 3) derive at least half of annual revenue from the selling of California residents' personal information. *Id.*

158. *See supra* notes 30–36 and accompanying text.

159. Jonathan "Yoni" Schenker, Michael F. Buchanan & Alejandro H. Cruz, *A Closer Look at the CCPA's Private Right of Action and Statutory Damages*, PATTERSON BELKNAP: DATA SEC. L. BLOG

Because data breach harms often come in difficult-to-quantify forms such as anxiety and preventative measures,[160] compensatory damages can be insufficient to make whole consumers whose data has been exposed. The CCPA provides for a limited private right of action following data breaches.[161] Significantly, this private right allows for statutory damages, relieving would-be plaintiffs of the often prohibitive burden of showing damages.[162] Because the CCPA guarantees a statutory award of between $100 and $750,[163] plaintiffs and their lawyers are more inclined to bring suit following data breaches, thereby holding corporations to account for their misuse, or poor protection of, private personal information.[164] In addition to the availability of statutory damages, consumers can request declaratory or injunctive relief following a data breach.[165]

California's enactment of the CCPA is indicative of a growing trend favoring strict state data privacy legislation.[166] Eighteen states, not including California, have introduced bills or initiated taskforces to overhaul state consumer privacy policies and regulations.[167] Two of these states, Maine and Nevada, have passed into law their own comprehensive data privacy acts.[168]

(Aug. 22, 2019), https://www.pbwt.com/data-security-law-blog/a-closer-look-at-the-ccpas-private-right-of-action-and-statutory-damages#:~:text=A%20Closer%20Look%20at%20the%20CCPA's%20Private%20Right%20of%20Action%20and%20Statutory%20Damages,-Categories%3A%20California%20Consumer&text=While%20consumers%20already%20had%20the,it%20provides%20for%20statutory%20damages [https://perma.cc/P835-5R2K].

160. *See supra* note 81 and accompanying text.

161. Christina H. Kroll, *CCPA: Consumers and the Right to Sue*, PROSKAUER: MINDING YOUR BUS. (May 31, 2019), https://www.mindingyourbusinesslitigation.com/2019/05/ccpa-consumers-and-the-right-to-sue/ [https://perma.cc/MY2T-ZW47]. Consumers who have fallen victim to a data breach can bring suit under the CCPA if they can show that the corporation did not "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." *Id.*; *see also* Alysa Zeltzer Hutnik, Lauri Mazzuchetti, Michael Lynch & Paul A. Rosenthal, *Be Careful What You Say About the CCPA*, KELLEY DRYE: AD LAW ACCESS (Nov. 12, 2019), https://www.adlawaccess.com/2019/11/articles/be-careful-what-you-say-about-the-ccpa/ [https://perma.cc/R8SA-87CK]; Schenker et al., *supra* note 162.

162. Schenker et al., *supra* note 162.

163. *Id.* (citing CAL. CIV. CODE § 1798.150(a)(1)(A)).

164. However, the right to statutory damages is not unlimited—the consumer must first give the corporation a right to "cure" its violations of the CCPA before it can file suit under the Act. If the corporation so cures, a plaintiff is no longer eligible for statutory damages should he/she decide to continue with the suit. *Id.*

165. Kroll, *supra* note 164.

166. *See* Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROS. (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/ [https://perma.cc/HA4X-MAJA]; *see also infra* Figure 1: State Privacy Legislation Comparison Chart.

167. *See* Noordyke, *supra* note 169; *see also infra* Figure 1: State Privacy Legislation Comparison Chart. Maryland and New Mexico are among those states that have introduced such consumer privacy legislation, though these bills have since been postponed indefinitely. *See infra* Figure 1: State Privacy Legislation Comparison Chart.

168. Noordyke, *supra* note 169; *see also infra* Figure 1: State Privacy Legislation Comparison Chart.

Maine's Act to Protect the Privacy of Online Customer Information ("PPOCI") is stricter than the CCPA in some ways and far more lenient in others.[169] While the CCPA protects all California residents, even those physically outside of the state, the Maine PPOCI only benefits those Maine citizens who are physically inside of the state of Maine and who are billed for broadband services received in Maine.[170] In addition, while the CCPA applies broadly to many out-of-state corporations that do business in California, only those broadband internet access services operating in Maine must comply with the PPOCI.[171] Significantly, the PPOCI does not specify how its regulations are to be enforced.[172] Though an amendment placing enforcement authority in the hands of the Maine Attorney General was introduced, that amendment did not pass.[173] Additionally, unlike the CCPA, the act does not authorize enforcement suits by private consumers.[174] Because it is unknown how the law will be enforced, the extent of its impact on consumer privacy in Maine and nationwide is unclear. However, should a Maine court read the act as authorizing a private right of action,[175] the PPOCI, like the CCPA would take a notable step towards protecting Americans' private information from data breaches and corporate malfeasance.[176]

Similarly, Massachusetts has introduced an expansive bill that would provide strong privacy protections for its consumers.[177] This bill would provide Massachusetts consumers the broadest privacy protections in the country.[178] For example, the bill inclusively defines "personal information" to cover "any information relating to an identified or identifiable consumer,"[179] and goes as far as to apply, not only to online identifying information, but also to "an individual's physiological, biological or

169. Lothar Determann & Helena J. Engfeldt, *Maine and Nevada's New Data Privacy Laws and the California Consumer Privacy Act Compared*, BAKER MCKENZIE (June 20, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/06/maine-and-nevada-new-data-privacy-laws [https://perma.cc/FNA3-2WSP].

170. *Id.*

171. *Id.*

172. *Id.*

173. *See* Peter Guffin & Kyle Noonan, *Maine's New Internet Privacy Law: What You Need to Know*, JD SUPRA (June 17, 2019), https://www.jdsupra.com/legalnews/maine-s-new-internet-privacy-law-what-48843/ [https://perma.cc/L4QB-J4EN].

174. *See id.*; Determann & Engfeldt, *supra* note 172.

175. Guffin & Noonan, *supra* note 176.

176. *See supra* notes 107–111 and accompanying text.

177. Michael R. Bertoncini, *Proposed Legislation in Massachusetts Would Create Private Right of Action for Improper Collection of Personal or Biometric Information*, JACKSON LEWIS: WORKPLACE PRIV. DATA MGMT. & SEC. REP. (Apr. 9, 2019), https://www.workplaceprivacyreport.com/2019/04/articles/consumer-privacy/proposed-legislation-in-massachusetts-would-create-private-right-of-action-for-improper-collection-of-personal-or-biometric-information/ [https://perma.cc/6YCK-JPMP].

178. *Id.*

179. *Id.*

behavioral characteristics."[180] Massachusetts' proposed bill would grant consumers a private right of action to enforce these regulations.[181] This right carries large statutory remedies and does not require that the consumer-plaintiff show actual injury to establish standing.[182] The bill specifies that "[a] violation of this chapter shall constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this chapter."[183] Under federal law, a statutory violation alone has generally been found insufficient to establish standing.[184] However, due to Massachusetts' more lenient standing requirements,[185] it is possible for the state to introduce such innovative legislation. Though Massachusetts' data privacy bill may never be signed into law, it exemplifies the kinds of legislative reforms that states can enact where the federal government is incapable, or unwilling, to regulate.

That the above states are contemplating passing, or have passed, vastly differing data privacy standards into law is telling. Should this pattern continue, it is possible that each of the fifty states could adopt their own unique legislation, causing confusion and inefficiency for businesses that operate on a national scale.[186] Businesses and industry groups are not unaware of the risks posed by a patchwork of differing state privacy laws.[187] Varying state consumer protection laws create a compliance nightmare for businesses that operate online across state lines.[188] For example, though Nevada and California share a border and a thriving interstate market, both

180. *Id.* This would include information like retina and iris scans, fingerprints, and voiceprints. *Id.*

181. *Id.*

182. *See id.*

183. S. 120, 191st Gen. Ct. § 9(a) (Mass. 2019).

184. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992) (finding that a statutory violation alone is insufficient to establish injury-in-fact). *But see* FEC v. Akins, 524 U.S. 11 (1998) (finding that a statutory violation of the FEC Act was alone sufficient to establish Art. III standing); *see also supra* notes 45–50 and accompanying text.

185. Massachusetts courts recognize a carve out in the state's standing doctrine for "public rights" cases. Sassman, *supra* note 149, at 373–74. Specifically, a public citizen has standing to sue in state court to compel the performance of a legally mandated duty. *Id.*

186. Gutter & Fields, *supra* note 145 ("[I]n the absence of a federal statute, it is possible that the growing number of nuanced state bills will be an administrative headache for companies that fall within the ambit of each state's laws.").

187. Esther Slater McDonald, *Industries Seek Uniform Federal Privacy Law to Preempt Inconsistent Patchwork of State Laws*, SEYFARTH: CONSUMER CLASS DEF. BLOG (July 15, 2019), https://www.consumerclassdefense.com/2019/07/industries-seek-uniform-federal-privacy-law-to-preempt-inconsistent-patchwork-of-state-laws/ [https://perma.cc/J7CS-8QNN]. In fact, twenty-seven industry groups petitioned Congress, requesting uniform federal privacy regulations to "provide certainty for businesses and consumers alike." *Id.*

188. Michael Beckerman, Opinion, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/73D2-TBFU].

states recently passed new privacy legislation that imposes different standards, such as when a consumer can opt out of having personal data sold.[189] These inconsistencies significantly raise compliance costs on businesses who operate, or even sell products or services in the interstate market.[190]

In addition, patchwork state privacy laws pose the added risk of giving consumers a false sense of security that their data is being protected. Journalist Michael Beckerman provides an illustrative example: "[A] California woman who orders an item from a Missouri business that manufactures in Florida could have her data regulated by three separate laws, or by no applicable law."[191] Consumers who interact with out-of-state businesses online have no way of knowing whether or not their personal data is being protected or which state's privacy laws, if any, will apply.[192]

A uniform state law would solve many of the problems this Note has raised. It would ensure consistent compliance standards among the states, while providing a regulatory framework in place to protect consumer's private data. In addition, states can venture where it seems the federal courts may not: a uniform state law could provide a private right of action so that citizens across the nation could take ownership of their rights to privacy and vindicate those rights on their own behalf.

CONCLUSION

This Note has proposed two solutions to the standing issues that surround the implementation of a private right of action for data breach harms. Both solutions have their virtues and their drawbacks, and this Note does not claim that one solution is more preferable than the other. However, as businesses and social relationships increasingly become features of an online world, it is important that the injuries that accrue from our online lives are seen for what they are. Certainly anxiety, emotional distress, pecuniary loss, and increased risk of future identity theft are injuries that "actually exist." It is simply a question as to how these injuries will be recognized and by whom.

Alyssa L. Aubuchon

189. *Id.*
190. *Id.*
191. *Id.*
192. *Id.*

193

State Comprehensive-Privacy Law Comparison

										Consumer Rights									Business Obligations							
State	Legislative Process							Statute/Bill (Hyperlinks)	Common Name	To Access to Collected	To Access to Shared	To Rectification	To Deletion	To Restriction	To Portability	To Opt-Out	Against Solely Automated Decision Making	Private Right of Action	Strict Age-based Opt-In	Notice/Transparency Requirement	Data Breach Notification	Risk Assessment	Prohibition on Discrimination	Purpose Limitation	Processing Limitation	Fiduciary Duty
California								**Ca. Civ. Code §§ 1798.100 - .199**	**California Consumer Privacy Act**	**x**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
~~Connecticut~~								~~RB 1108/SB 1108~~																		
Hawaii								*SB 418* [i]		*x*	*x*		*x*		*x*	*x*			*16*	*x*	*x*		*x*			
~~Hawaii~~								~~HCR 225~~																		
Illinois								*HB 3358*	*Data Transparency and Privacy Act*		*x*					*x*				*x*						
~~Louisiana~~								~~HB 249~~																		
Maine								**LD 946** [ii]	**An Act To Protect the Privacy of Online Consumer Information**					**x**		**in**				**x**			**x**			
~~Maryland~~								~~SB 613~~	~~Online Consumer Protection Act~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~				~~x~~			~~x~~			
Massachusetts								*SD 341/S 120*		*x*	*x*		*x*		*x*	*x*		*x*	*18*	*x*			*x*			
Minnesota								*HF 2917/SF 2912*		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*		*x*			*x*	
Nevada								**SB 220/Chapter 603A**								**x**				**x**	**x**					
New Jersey								*S2834*			*x*					*x*				*x*			*x*			
~~New Mexico~~								~~SB 176~~	~~Consumer Information Privacy Act~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~		~~s~~	~~18~~	~~x~~			~~x~~			
New York								*SB S5642* [iii]	*New York Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*		*x*	*x*				*x*	*x*
~~North Dakota~~								~~HB 1485~~																		
Pennsylvania								*HB 1049*	*Consumer Data Privacy Act*	*x*	*x*		*x*			*x*		*s*	*16*	*x*			*x*			
Rhode Island								*HB 5930/S0234*	*Consumer Privacy Protection Act*	*x*	*x*		*x*		*x*	*x*		*x*	*16*	*x*			*x*			
~~Texas~~								~~HB 4390~~ [iv]	~~Texas Privacy Protection Act~~																	
Washington								*SB 5376*	*Washington Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*	*x*	*x*				

In Session: MA, NJ, PA

Introduced | In Committee | Crossed Chamber | Cross Committee | Passed | Signed

Bold - passed law
Italics - proposed bill, not passed
s - private right of action for security violations only
in - opt-in consent requirement

~~Black strikethrough - bill postponed indefinitely~~
~~Purple strikethrough - task force substituted for comprehensive bill~~

[i] Hawaii SB 418 is pending while the task force has been adopted.
[ii] Maine LD 946 applies only to internet service providers.
[iii] New York SB S5642 includes a broad consumer right to opt-out of any processing, not just the sale of personal information.
[iv] Texas HB 4390 is a GDPR-style restriction-based bill that prohibits a business from collecting or processing information except under certain circumstances.

Legislative Process: Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

iapp

Last updated: 10/15/2019

Figure 1: State Privacy Legislation Comparison Chart

193. Noordyke, *supra* note 169.