STANDING A CHANCE: DOES *SPOKEO* PRECLUDE CLAIMS ALLEGING THE VIOLATION OF CERTAIN STATE DATA BREACH LAWS?

Taryn Elliott[*]

I. INTRODUCTION

American standing jurisprudence, which determines what cases may be brought in federal court, arises from the "case or controversy" requirement of the United States Constitution.[1] As the Supreme Court has interpreted it, this provision prohibits Article III courts from hearing lawsuits unless the issue raises and alleges a sufficient injury-in-fact, establishes causation, and allows for redressability by the court.[2]

The question of whether Congress can define "injury-in-fact," and therefore confer standing via statutory language, has been the subject of much inquiry and debate throughout the years, as legislatures have increasingly included so-called "citizen suit" or "private right of action" provisions in enacted laws to allow individuals to bring suit.[3] The recent Supreme Court decision in *Spokeo v. Robins* is perceived to have cut away at the validity of certain federal statutory provisions that allow individuals to bring suit when their sole claims are that the statute was violated.[4] In the *Spokeo* case, the Court assessed a plaintiff's standing to sue based on a violation of the federal Fair Credit Reporting Act (FCRA) and held that "a bare procedural violation, divorced from any concrete harm" does not satisfy the injury-in-fact requirement.[5]

[*] J.D. Candidate, 2019, Seton Hall University School of Law; B.A., 2011, Rutgers University.

[1] U.S. CONST. art. III, § 2.

[2] Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

[3] Cass R. Sunstein, *What's Standing After Lujan? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163 (1992) (discussing the view that prior to *Lujan*, the unanimous view of the lower courts had been that a legislative grant of citizen standing was constitutional, even without a showing of injury-in-fact).

[4] Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Francis X. Riley III, *What You Should Know About "Standing" Since Spokeo*, INSIDEARM (June 19, 2017), https://www.insidearm.com/news/00043021-what-you-should-know-about-standing-spoke/.

[5] *Spokeo*, 136 S. Ct. at 1549.

In the wake of the 2016 *Spokeo* decision, courts have analyzed standing in the context of alleged federal statutory violations differently, depending on which laws the plaintiffs claim have been violated.[6] It is also unclear if and how *Spokeo* will impact class action lawsuits brought based on state law claims, and since certain federal courts in recent years have certified nationwide classes under the law of a single state, this question may have major implications for individuals alleging state statutory violations in a national class action suit.[7]

One area where federal courts may soon determine congressional authority to define injuries concerns the increasingly pervasive issue of data breaches. In recent years, the United States has seen a number of high-profile breaches, which are often defined as incidents "in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve payment card information (PCI), personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property."[8] Among the most recent and highest-impact instances are the 2013 Target breach, in which 40 million credit and debit card accounts, as well as data on 70 million customers were compromised;[9] the 2014 Home Depot breach, where 56 million credit card accounts and 53 million email addresses were stolen;[10] and the 2015 Anthem data breach, in which 80 million patient and employee records were obtained.[11] Arguably, however, the most concerning data breach took place in 2017, when the personal information, including Social Security numbers and addresses, of up to 143 million Americans was stolen from the consumer credit reporting agency Equifax.[12] Given the increasing threat of cyber-attacks and data breaches, individuals have sought to bring class action suits to hold the companies who released their data accountable for their failure to protect the information. These litigants often allege, among other things, that the company that experienced the data breach failed to comply with state data breach notification laws and state

[6] Riley, *supra* note 4.

[7] *See* Pecover v. Elec. Arts, Inc., 633 F. Supp. 2d 976 (N.D. Cal. 2009); *see also* Jane E. Willis & Anne E. Johnson, *Certification of a National Class Under State Law: Is Electronic Arts a Trend or an Outlier?*, BLOOMBERG L. REP. (Mar. 1, 2011), https://www.ropesgray.com/newsroom/alerts/2011/03/certification-of-a-national-class-under-state-law-is-electronic-arts-a-trend-or-an-outlier.aspx.

[8] Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Apr. 6, 2018), https://digitalguardian.com/blog/history-data-breaches.

[9] Allison Ross, *11 Data Breaches that Stung US Consumers*, BANKRATE (Sept. 9, 2015), https://www.bankrate.com/finance/banking/us-data-breaches-1.aspx#slide=1.

[10] *Id.*

[11] *Id.*

[12] Kaya Yurieff, *Equifax Data Breach: What You Need to Know*, CNN (Sept. 10, 2017), http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/.

consumer protection laws.[13] Under the *Spokeo* standard, however, failure to comply with state data breach laws may not be sufficient to allege injury-in-fact to obtain standing to sue. This is especially true if courts do not find that post-breach claims are harmful enough under a recent standard set forth in *Clapper v. Amnesty International USA*, which requires that injury be "certainly impending."[14] Given the nature of data breaches and the type of injury that is typically suffered after an incident occurs, this Comment argues that *Spokeo* should not bar litigation where failure to comply with data breach laws is alleged as a standalone claim, because it is not merely a "bare procedural violation,"[15] and failure to comply causes real harm.

Part II of this Comment discusses the history of cases leading to *Spokeo* and the test for determining that standing has been established. Part III addresses the nature of the injury that individuals tend to experience after a data breach occurs, and why the issue presents a unique challenge for courts when determining standing. Part IV discusses the purpose of private right of action provisions in state data breach laws, and how state legislators intended to create a right in these statutes. Part V analyzes how the harm that flows from the violation of a data breach statute is similar to tort liability. Part VI discusses the current circuit split post-*Spokeo* regarding whether private right of action provisions can confer Article III standing, and why the issue should be resolved in favor of upholding statutory standing in the data breach context.

II. THE WINDING PATH TO *SPOKEO* AND THE CURRENT TEST FOR STANDING

In the 1992 case of *Lujan v. Defenders of Wildlife*, the Supreme Court first tackled the question of whether Congress could confer standing.[16] In the majority opinion, Justice Scalia suggested that in order for a private right of action provision to create an injury-in-fact, the Constitution requires a certain type of personal injury, akin to those at common law, for standing.[17] "This decision is believed to have invalidated a large number of statutes in which Congress has attempted to use the 'citizen-suit' device as a mechanism for controlling unlawfully inadequate enforcement of the law."[18] Justices Kennedy and Souter in their *Lujan* concurrence, however, stated that

---

[13] Al Saikali, *The Target Data Breach Lawsuits: Why Every Company Should Care*, DATA SECURITY L. J. (Dec. 30, 2013), http://www.datasecuritylawjournal.com/2013/12/30/the-target-data-breach-lawsuits-why-every-company-should-care/.

[14] Clapper v. Amnesty Int'l, 568 U.S. 398, 411 (2013).

[15] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549–50 (2016).

[16] Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

[17] *Id.*

[18] Sunstein, *supra* note 3, at 165.

congressionally enacted citizen standing provisions may be constitutional as long as they are specific about the nexus between the injury and the class of citizens authorized to bring suit under the law.[19] *Lujan* is thus believed to have rejected the use of private cause of action provisions in circumstances that are deemed too far removed from any personal injury to the plaintiff, but the case left open the question of whether such provisions may be enforceable to confer standing when the individual(s) challenging the statutory violation suffered some type of harm as a result of the violation.

In the time between the *Lujan* decision in 1992 and the *Spokeo* decision in 2016, the issue of federal statutory standing without "actual injury" had been decided inconsistently among the federal circuit courts. The Sixth Circuit, for instance, held in the 2009 case of *Beaudry v. TeleCheck Services, Inc.*[20] that a plaintiff could bring an action under the FCRA without showing actual harm.[21] Similarly, the Eighth Circuit heard the case of *Charvat v. Mutual First Federal Credit Union*,[22] where the plaintiff alleged the violation of the Electronic Funds Transfer Act without demonstrating actual injury.[23] On the other hand, the Second Circuit denied standing in the 2009 case of *Kendall v. Employees Retirement Plan of Avon Products*,[24] and the Fourth Circuit later declined to hear the case of *David v. Alphin*,[25] holding that plaintiffs do not have standing to bring claims alleging the violation of ERISA without showing actual injury.[26]

In the Court's decision in *Spokeo v. Robins*, in which the plaintiff alleged a violation of the FCRA, the Supreme Court held that the plaintiff did not have standing unless he suffered "concrete" and "particularized" harm in light of the defendant's conduct in violation of the FCRA.[27] Although the Court denied standing to the plaintiff in *Spokeo* for "bare procedural violations" of federal statutes, without more,[28] it did not close the door entirely to plaintiffs seeking to bring suit based on a statutory violation.[29] The Court set forth a test that courts may consider in future cases

19 *Lujan*, 504 U.S. at 579.

20 579 F.3d 702 (6th Cir. 2009).

21 David J. Lender, Eric S. Hochstandy & Gregory Silbert, *Supreme Court to Decide Whether Plaintiffs Have Standing to Bring Class Action Lawsuits Without Proof of Actual Injury*, LEXOLOGY (July 6, 2015), https://www.lexology.com/library/detail.aspx?g=b595d8b7-17b8-4624-8eef-1a53bdc23ea5.

22 725 F.3d 819 (8th Cir. 2013).

23 Lender, Hochstandy & Silbert, *supra* note 21.

24 561 F.3d 112 (2d Cir. 2009).

25 704 F.3d 327 (4th Cir. 2009).

26 Lender, Hochstandy & Silbert, *supra* note 21.

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

28 *Id.*

29 *Id.*

to evaluate whether the violation of a statute establishes concrete injury.[30] "First . . . it is instructive to consider whether an 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,"[31] and "[s]econd . . . whether Congress created a procedural or substantive right in the statute at issue."[32]

Since *Spokeo*, federal courts have determined the existence of an injury-in-fact on a case-by-case basis when the litigants claim that a federal statute has been violated.[33] In addition, recent federal circuit court decisions have addressed a litigant's standing to bring claims under state law in federal court, and whether state statutory private right of action provisions can confer standing (though federal provisions presumably cannot if they are divorced from actual injury or harm).[34] Given the fact that state statutes largely dictate how a holder of information must react when a data breach occurs, it is possible that the application of *Spokeo* to state statutory claims will be decided by the Supreme Court in the years to come.

III. THE HARM THAT FLOWS FROM DATA BREACHES AND HOW COURTS INTERPRET THAT HARM

To meet the requirements for injury-in-fact to obtain Article III standing, plaintiffs must show that they have experienced an injury that is imminent and not "too speculative,"[35] and that the injury suffered was "concrete" and "particularized."[36] Courts have struggled with data breach harm because, by their nature, the harms are "intangible, risk-oriented, and diffuse,"[37] and "[t]hese characteristics are areas that have been particularly vexing for courts."[38] The reality of the world of data breaches is that harm can be recognized many years in the future when data is used long after it

30 *Id.*

31 Matera v. Google Inc., No. 15-cv-04062, 2016 WL 5339806, at *9 (N.D. Cal. Sept. 23, 2016).

32 *Id.*

33 Simon A. Fleischmann, P. Russell Perdew & Chethan G. Shetty, *Spokeo v. Robins: Supreme Court Rejects Article III Standing Based Solely on Statutory Violation*, LOCKE LORD (May 16, 2016), http://www.lockelord.com/newsandevents/publications/2016/05/~/media/7A16BC949D064067A55198B548FDCD00.ashx.

34 Ronnie Solomon, *Post-Spokeo, Standing Challenges Remain Unpredictable*, LAW360 (Oct. 26, 2016), https://www.law360.com/articles/854898/post-spokeo-standing-challenges-remain-unpredictable.

35 Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013).

36 *Id.*

37 Daniel Solove, *When Do Data Breaches Cause Harm?*, TEACH PRIVACY: PRIVACY & SECURITY BLOG (Dec. 28, 2016), https://www.teachprivacy.com/when-do-data-breaches-cause-harm/.

38 *Id.*

has been obtained. Therefore, the issue of harm is different for plaintiffs in this context than for plaintiffs who bring suit solely based on statutory violations that are completely separate from any personal injury that they have experienced at the time. Accordingly, the *Spokeo* holding should not bar plaintiffs from bringing suit to challenge the violation of state data breach laws simply because the violation has not yet "harmed" them in the more commonly understood sense of the word.

As many experts in the field of data security have noted, the harm that flows from a data breach takes place largely in the future, as opposed to the present. Breaches "open the door for total identity theft," says Robb Reck, Chief Information Security Officer at Ping Identity,[39] and the data that is compromised during these incidents "will be used for years" according to Avivah Litan, a security analyst.[40] "Data theft poses an indefinite threat of future harm, as birthdate, full name and social security number remain a skeleton key of identity in many systems."[41] In addition to the risk of hackers using individuals' data in the future, breaches cause other types of damages to individuals who are impacted, as "[m]any are worried about doing the digital-era equivalent of constantly looking over their shoulder, waiting for someone to appropriate their identity, or dredge up some intimate, haunting secret they thought was long buried."[42]

State and federal legislatures and executive branches have also acknowledged the nature of the harm that individuals may experience after their data has been breached over the years. As the Federal Trade Commission (FTC) has noted, "[p]eople whose identities have been stolen can spend months or years—and thousands of dollars—cleaning up the mess the thieves have made of a good name and credit record."[43] The FTC also notes that "victims of identity theft may lose job opportunities, be refused for loans, and even get arrested for crimes they didn't commit. Humiliation, anger, and frustration are among the feelings victims experience."[44] As discussed during the enactment of New Hampshire House Bill 1660 in 2006, one of the first data breach notification laws in the country, "[m]ost victims

---

[39] Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA TODAY (Sept. 9, 2017, 10:08 AM), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/.

[40] *Id.*

[41] Farai Chideya, *Data Theft Today Poses Indefinite Threat of "Future Harm"*, THE INTERCEPT (June 12, 2015, 12:26 PM), https://theintercept.com/2015/06/12/data-breach-threat-of-future-harm/.

[42] *Id.*

[43] *Take Charge: Fighting Back Against Identity Theft*, MYCOLLEGEMONEYPLAN 1 (2006), http://www.mycollegemoneyplan.org/sites/default/files/documents/Take%20Charge%20Fighting%20Back%20Against%20ID%20Theft.pdf.

[44] *Id.*

don't find out what has happened until long afterward, when they're called by a collection agency or turned down for a loan."[45]

Since the harm from a data breach is more likely to occur in the future, however, courts have grappled with whether litigants whose data has been compromised meet the requirements for standing. The most high-profile data breach cases are typically filed in federal court as class action suits and are often settled by the parties. For example, in the wake of the Anthem data breach, "[m]ore than 100 data breach class action lawsuits were filed . . . alleging [that] Anthem failed to adequately safeguard the personal information of subscribers and failed to adequately notify those whose personal information was compromised" in accordance with state data breach laws.[46] The Anthem cases were ultimately consolidated and settled, and the company paid $115 million to approximately 78 million class members.[47] Similarly, settlements for class actions filed against Home Depot and Target after the companies experienced data breaches were approved in 2016[48] and 2015,[49] respectively, and the companies each paid tens of millions of dollars to the plaintiffs.

When suing a company after a data breach has occurred, plaintiffs bring many different types of claims. In the United States, companies that experience large breaches typically face class action lawsuits,[50] and "common claims in such lawsuits are that the company violated state unfair business practices laws, breached a contract, was negligent, or is subject to liability for a privacy tort."[51] Plaintiffs have also sought to assert claims based on federal laws in the wake of a data breach.[52] Faced with these numerous cases in recent years, courts have ruled differently regarding the likelihood of future harm after a data breach, and whether that harm was

---

45 H.B. 06-2049, 1st Sess., at 59 (N.H. 2005).

46 Anne Bucher, *Judge Orders Gov't to Produce Docs in Anthem Data Breach Class Action*, TOP CLASS ACTIONS (Feb. 24, 2017), https://topclassactions.com/lawsuit-settlements/lawsuit-news/499111-judge-orders-govt-produce-docs-anthem-data-breach-class-action/.

47 Bodweya Tweh, *Anthem Agrees to $115 Million Settlement of Data Breach Lawsuit*, FOX BUS. (June 23, 2017), http://www.foxbusiness.com/features/2017/06/23/anthem-agrees-to-115-million-settlement-data-breach-lawsuit.html.

48 Tara Seals, *Home Depot to Pay $27.25m in Latest Data Breach Settlement*, INFO SECURITY MAG. (Mar. 13, 2017), https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/.

49 Samantha Masunaga, *Target Will Pay $18.5 Million in Settlement with States Over 2013 Data Breach*, L.A. TIMES (May 23, 2017, 3:00 PM), http://www.latimes.com/business/la-fi-target-credit-settlement-20170523-story.html.

50 Ffion Flockhart, Steve Tenai & Andrew L. Hoffman, *Civil Litigation Risks Following Data Breaches*, FINANCIER WORLDWIDE (June 2015), https://www.financierworldwide.com/civil-litigation-risks-following-data-breaches/#.WbvwD2NpLY4.

51 *Id.*

52 *Id.*

sufficient to establish injury-in-fact.

The first significant case dealing with standing in the data breach context was *Krottner v. Starbucks*, where the court held that the increased threat of theft of personal data on a stolen laptop did confer standing.[53] Following *Krottner*, however, the Supreme Court's 2013 decision in *Clapper v. Amnesty International* introduced a higher standard for assessing potential harm, providing that a possible future injury that was "certainly impending" may suffice as an injury-in-fact.[54] Following *Clapper*, many courts have declined to confer standing to individuals whose data was compromised, finding that the future harm alleged was too speculative.[55] This unwillingness to confer standing is not uniform, however, and some courts have allowed cases to proceed when the harm alleged is simply that the plaintiff's data was compromised, or that the plaintiff's injuries are of the type that most experience in the aftermath of a data breach. For example, in the Target data breach litigation in a Minnesota federal court, Judge Magnuson found that the plaintiffs had sufficient injuries for standing purposes because they suffered costs "including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills and late payment charges or new card fees."[56] Despite Target's attempts to argue that plaintiffs must allege a more concrete injury, like the closure of their bank accounts, Magnuson stated that these arguments "set a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage."[57] In addition, the Seventh Circuit and Third Circuit courts upheld the assertion of harm and granted standing to individuals whose data had been breached in the Neiman Marcus[58] and Horizon[59] data breach cases, respectively.

It appears, then, that courts may be becoming more familiar with how injury manifests in the context of large data breaches, and that judges may be increasingly receptive to the arguments that individuals impacted by a

---

53 Krottner v. Starbucks, 628 F.3d 1139, 1143 (9th Cir. 2010); Stephen E. Embry, *Data Breach Litigation: The Sky Is Falling or a Failure of Proof?*, CLASS COUNS. BLOG (Aug. 14, 2015), https://www.linkedin.com/pulse/data-breach-litigation-sky-falling-failure-proof-stephen-embry/.

54 Clapper v. Amnesty Int'l, 568 U.S. 398, 408–10 (2013).

55 Embry, *supra* note 53.

56 Embry, *supra* note 53; *see also In re* Target Corp. Customer Data Breach Sec. Litig., 64 F. Supp. 3d 1304 (D. Minn 2014).

57 Kaleigh Simmons, *Everything You Need to Know About the Target Data Breach Lawsuits*, RIPPLESHOT (Feb. 4, 2015, 7:00 AM), http://info.rippleshot.com/blog/everything-you-need-to-know-about-the-target-data-breach-lawsuits.

58 Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015); John K. Higgins, *Consumers Gain More Power to Seek Data Breach Damages*, E-COM. TIMES (Aug. 21, 2017), http://www.ecommercetimes.com/story/84747.html.

59 *In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639–40 (3d Cir. 2017).

data breach will suffer harm that is "certainly impending" under the *Clapper* standard. "Many courts seem to recognize the suggestion raised in the Neiman Marcus case that the entire reason the hackers are trying to steal the personal information is to try to accomplish an identity theft, and that sooner or later hackers with access to the information will try."[60] For instance, "[t]he D.C. Circuit recently embraced the premise that the risk of future harm can be enough to meet the *Spokeo* standing bar in a data breach case involving health insurer CareFirst."[61] This decision "deepen[ed] a circuit split that's been fueled in part by judges' growing familiarity with how such intrusions play out."[62] The ever-growing number of data breach occurrences has also placed pressure on the judiciary to find solutions and remedies for those who fear what might happen to them after their private, personal data has been compromised.[63] Given that courts have decided differently regarding the underlying claim of harm suffered from a data breach and whether that is sufficient to confer standing under the *Clapper* standard, it is all the more important that courts recognize that claims under private right of action provisions in state data breach laws provide a way into court, and are not barred as procedural violations under the *Spokeo* standard.

An understanding of how harm occurs after a data breach is slowly reaching the federal courts. When drafting state data breach laws, however, many legislators and regulators arguably already understood the harm that could take place and therefore inserted provisions to allow individuals whose data is compromised to file suit.

IV. THE PURPOSE OF STATE DATA BREACH LAWS AND PRIVATE RIGHT OF ACTION PROVISIONS

Legislative private right of action provisions grant private actors the right to sue if another private actor violates the law in which the provision appears.[64] Generally, the purpose of private right of action or citizen suit provisions in legislation historically has been to ensure that regulated entities comply with the law as set forth by the legislature by allowing a private party

---

60 Kevin LaCroix, *Deepening Circuit Split on Data Breach Suit Standing*, D&O DIARY (Aug. 6, 2017), http://www.dandodiary.com/2017/08/articles/cyber-liability/deepening-circuit-split-data-breach-suit-standing/.

61 Allison Grande, *Data Breach Suits Find Easier Path with DC Circ. Ruling*, LAW360 (Aug. 3, 2017), https://www.law360.com/insurance/articles/951179/data-breach-suits-find-easier-path-with-dc-circ-ruling.

62 *Id.*

63 Embry, *supra* note 53.

64 Daniel Edelson, *What Is an Implied Private Right of Action?*, USLAWESSENTIALS, http://uslawessentials.com/20141116what-is-an-implied-private-right-of-action/ (last visited Jan. 10, 2018).

to "enforce a regulatory standard."[65] "With a number of devices, including the citizen suit, Congress hoped to overcome administrative laxity and unenthusiasm, and also to counteract the relatively weak political influence of beneficiaries."[66] In addition, "[p]romoting the purpose of a statute through citizen initiative is an important policy goal behind a private right of action."[67] In the absence of a private right of action, the Attorney General or another appropriate state agency typically oversees the enforcement of state statutes.[68] State legislators have included private right of action provisions to allow private citizens impacted by a statutory violation to police compliance with the law by bringing suit.

Since California's enactment of the country's first data breach notification bill in 2003,[69] all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed laws that require companies that retain an individual's personal information to disclose when that information has been breached.[70] While no state law is identical, there are many provisions that address similar issues in the bills that have been enacted. "Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc)."[71] The laws also frequently include "definitions of 'personal information' (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.);[72] what constitutes a breach (e.g., unauthorized acquisition of data);[73] requirements for notice (e.g., timing or method of notice, who must be notified);[74] and exemptions (e.g., for

---

65 William H. Timbers & David A. Wirth, *Private Rights of Action and Judicial Review in Federal Environmental Law*, 70 CORNELL L. REV. 403, 404 n.6 (1985).

66 Sunstein, *supra* note 3, at 193 (discussing the view that prior to *Lujan*, the unanimous view of lower courts had been that a legislative grant of citizen standing was constitutional even without a showing of injury-in-fact).

67 Timbers & Wirth, *supra* note 65.

68 Kymberly Kochis, Veronica Wayner & Alex Fuchs, *Understanding and Defending State Consumer Protection Actions*, SUTHERLAND 1, 14 (Sept. 29, 2016), https://us.eversheds-sutherland.com/portalresource/UnderstandingandDefendingStateConsumerProtectionActions.pdf.

69 Ryan J. Udell, Shari G. Pressman & Wasim S. Rahman, *Data Breach—What You Need to Know Now: California's Data Security Breach Notification Law*, WHITE & WILLIAMS LLP (Oct. 7, 2011), https://www.whiteandwilliams.com/resources-alerts-California-Data-Security-Breach-Law.html.

70 *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.
aspx. (last updated Sept. 29, 2018).

71 *Id.*

72 *Id.*

73 *Id.*

74 *Id.*

encrypted information)."[75] Some laws also include safe harbor provisions that allow entities to forego notification of a breach in certain circumstances.[76]

In addition to these provisions, fifteen states specifically provide for a private right of action in their data breach laws, which allow a suit to be brought if the notification statutes are not complied with.[77] Further, a "short but growing list of states . . . require entities to provide some form of credit monitoring services after a breach."[78] These additional provisions suggest that state legislators understand the harm that can come from a data breach, and that an individual must be notified when a breach takes place and provided with options to help them address and mitigate their resulting injuries. This intent is clear in many cases, including when reviewing the history of the first data breach law in the United States, California Senate Bill 1386. According to its author, the bill was "intended to help consumers protect their financial security by requiring any agency or business that maintains a computerized data system that contains personal information to disclose any breach of the security of the system immediately . . . ."[79] The notification would be required "if the information disclosed could be used to commit identity theft."[80] In addition, the enacted law states that "[a] consumer injured by a violation of the provisions of this bill would have the right to bring civil suit and recover damages."[81] At the time the legislation was being considered, supporters of the bill argued that the bill was necessary because consumers needed to know about a breach of their information security so that they could take effective steps to prevent identity theft.[82] The passage of this legislation, which required disclosure of data breaches and included a private right of action provision,[83] undoubtedly

---

[75] *Id*.

[76] *See* Jennifer J. Hennessey et al., *State Data Breach Notification Laws*, FOLEY & LARDNER LLP (May 21, 2018), https://www.foley.com/state-data-breach-notification-laws/.

[77] Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A. (May 2016), https://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html.

[78] Caleb Skeath, *Delaware Amends Data Breach Notification Law to Require Credit Monitoring, Attorney General Notification*, NAT'L L. REV. (Aug. 29, 2017), https://www.natlawreview.com/article/delaware-amends-data-breach-notification-law-to-require-credit-monitoring-attorney.

[79] *An Act to Amend, Renumber, and Add Section 1798.82 of, and to Add Section 1798.29 to, the Civil Code, Relating to Personal Information: Hearing on S.B. 1386 Before the Assembly Judiciary Comm.*, 2002 Leg., Sess. 1386 (Cal. 2002).

[80] *Id*.

[81] CAL. CIV. CODE § 1798.84(b) (West 2010).

[82] *An Act to Amend, Renumber, and Add Section 1798.82 of, and to Add Section 1798.29 to, the Civil Code, Relating to Personal Information: Hearing on S.B. 1386 Before the Assembly Judiciary Comm.*, *supra* note 79.

[83] CIV. § 1798.84(b).

helped citizens to avoid harm because they learned about numerous instances of theft of their private data, which they likely would not have known about but for the law being in place. "Because of SB 1386, we learned in 2005 that ChoicePoint—a company most Americans had never heard of—had somehow sold detailed credit histories on more than 163,000 consumers directly to identity thieves."[84] "And in 2007, we learned that identity thieves had broken into the computer systems of the discount retailer TJX and stole[] more than 45 million credit-card numbers."[85] Failure to disclose a breach or comply with state data breach notification laws can clearly harm individuals who would not otherwise be aware of the fact that their data had been exposed and could not take the proper precautions afterward to protect themselves from misuse of their data.

Not long after California, the Washington legislature also enacted a data breach notification statute, Senate Bill 6043, which included a private right of action providing that "[a]ny customer injured by a violation of this section may institute a civil action to recover damages."[86] As these bills moved through state legislatures, members noted that "[v]ictims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative."[87] It appears from the various legislative histories surrounding data breach laws that state legislatures enacted data breach notification bills to address the harm that occurs to consumers when they are not made aware of the fact that their data has been stolen. In a letter from New Hampshire Governor John Lynch to Representative Sheila Francoeur regarding the state's data breach notification law, which includes a private right of action provision, Governor Lynch noted that "[b]y requiring prompt disclosure of security breaches, our citizens will be in a better position to react in a timely manner to potential threats against the misuse of their identities."[88] Recently, the California legislature reinforced the importance of including a private right of action in data breach notification laws by retaining the provision allowing individuals to bring suit and providing for a specified range of statutory damages in its amended and updated 2018 version of the law.[89] It

84 Simson Garfinkel, *Privacy Requires Security, Not Abstinence*, MIT TECH. REV. (June 23, 2009), https://www.technologyreview.com/s/414015/privacy-requires-security-not-abstinence/.

85 *Id*.

86 *An Act Relating to Breaches of Security That Compromise Personal Information,* S.B. 6043, 2005 Leg., Sess. 1, 3 (Wash. 2005).

87 *An Act to Amend, Renumber, and Add Section 1798.82 of, and to Add Section 1798.29 to, the Civil Code, Relating to Personal Information: Hearing on S.B. 1386 Before the Assembly Judiciary Comm.*, *supra* note 79.

88 Letter from John Lynch, Governor, N.H., to Sheila Francoeur, Representative, N.H. (Jan. 10, 2006) (on file with the New Hampshire General Court).

89 Assemb. B. 375, 2018 Leg., Reg. Sess. (Cal. 2018).

is clear that in California, Washington, and New Hampshire, legislators understand the harm that could occur to citizens when the notification law is not complied with, and this is likely why they included private right of action provisions to allow these individuals to bring suit based on this harm.

A recent occurrence highlights the importance of allowing individuals to bring suit after their data has been breached. As a result of the Equifax breach, "the private financial and personal details of as many as 143 million Americans have been exposed to hackers."[90] A class action lawsuit, *Allen et al. v. Equifax*, was filed, and among the claims is the company's delay in informing consumers about the breach, "thereby preventing them from taking steps to minimize the damage."[91] The allegations charged "include violations of . . . state consumer protection laws as well as rules regarding deceptive practices and data breaches, all of which are recounted in the 323-page filing."[92] The recent Equifax breach, and resulting reaction from both state and federal legislators throughout the country, reinforces the notion that legislators intend to hold companies accountable for failure to notify citizens of a breach of their data. After the breach, Senator Robert Menendez of New Jersey stated that it is "outrageous that Equifax waited more than a month to inform consumers about this hack."[93] During a congressional hearing, Representative Markwayne Mullin of Oklahoma told the former CEO of Equifax that the company's response "should have been like a fire alarm on the wall, ready at a moment's notice to be pulled."[94] There have also been numerous efforts over the years to enact one federal data breach standard, as opposed to the patchwork of fifty state laws, including the Personal Data Notification and Protection Act.[95] "Under this proposed legislation, Equifax would have had to disclose its breach within 30 days—not the six weeks it took—to the FTC and the Department of Homeland Security."[96] The

[90] Bryce Covert, *Get Rid of Equifax*, N.Y. TIMES (Sept. 21, 2017), https://www.nytimes.com/2017/09/21/opinion/get-rid-of-equifax.html.

[91] Kenneth R. Harney, *Data Breach at Equifax Prompts a National Class-Action Suit*, WASH. POST (Nov. 22, 2017), https://www.washingtonpost.com/realestate/data-breach-at-equifax-prompts-a-national-class-action-suit/2017/11/20/28654778-ce19-11e7-a1a3-0d1e45a6de3d_story.html?utm_campaign=0618182381-EMAIL_CAMPAIGN_2017_11_27&utm_medium=email&utm_source=I.I.I&utm_term=.291c07336ab4.

[92] *Id.*

[93] Press Release, Sen. Bob Menendez, What You Should Know About Equifax Data Breach (Sept. 14, 2017).

[94] Jim Puzzanghera, *'I Don't Think We Can Pass a Law That Fixes Stupid': Lawmakers Berate Equifax Ex-CEO*, L.A. TIMES (Oct. 3, 2017), http://www.latimes.com/business/la-fi-equifax-hearing-ceo-20171003-story.html.

[95] Christopher Mims, *Should the U.S. Require Companies to Report Breaches*?, FOX BUS. (Sept. 24, 2017), http://www.foxbusiness.com/features/2017/09/24/should-u-s-require-companies-to-report-breaches.html.

[96] *Id.*

concern about timely notification of data breaches is one of the main motivators for enacting, and ensuring compliance with, state laws. Last year, "Equifax Inc. learned about [the] major breach of its computer systems in March—almost five months before the date it [had] publicly disclosed," according to Bloomberg News.[97] "New questions about Equifax's timeline are also likely to become central to the crush of lawsuits being filed against the Atlanta-based company."[98] Equifax's failure to disclose this first breach caused clear harm to those whose data was later acquired in the second breach and those who were not given the opportunity to adequately protect themselves in light of the first threat. Individuals could have been spared harm if Equifax had conducted an investigation of the first breach that was "sufficiently thorough" and not "closed too soon," thereby requiring them to notify more individuals of the incident.[99] The purpose of requiring companies to disclose breaches in accordance with state law is to ensure that individuals are not harmed by the failure to be informed of a breach. The Equifax issue highlights how this harm can occur.

Even in states that do not have a private right of action provision in their data breach laws, courts impliedly recognize that there is a legislative intent behind those that do. For instance, in dismissing a Pennsylvania class action suit, Judge R. Stanton Wettick, Jr. stated that the court refused to interfere with the legislature's direction in this area of the law where they had not provided a private right of action to bring suit after a data breach occurred.[100] Further, even post-*Spokeo*, recent federal court decisions have affirmed the idea that private rights of action imply a legislative intent to confer standing with regard to privacy issues. In discussing the FCRA, the court hearing the case of the recent Horizon data breach stated that "[Congress] created a private right of action to enforce the provisions of FCRA . . . which clearly illustrates that Congress believed that the violation of FCRA causes a concrete harm to consumers."[101] The court found legislative intent implied from the language of the FCRA, which provides for a capped amount of

---

[97] Michael Riley, Anita Sharpe & Jordan Robertson, *Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed*, BLOOMBERG (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack earlier-than-the-datedisclosed?utm_source=I.I.I.+Daily+Newsletter&utm_campaign=c90b b06d51EMAIL_CAMPAIGN_2017_09_19&utm_medium=email&utm_term=0_092139a76 a-c90bb06d51-122523861.

[98] *Id.*

[99] *Id.*

[100] *Pennsylvania State Court Rejects Data Breach Claims*, FOX ROTHSCHILD LLP (June 10, 2015), https://dataprivacy.foxrothschild.com/2015/06/articles/data-protection-law-compliance/pennsylvania-state-court-rejects-data-breach-claims/.

[101] *See In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017).

statutory damages following willful violations of the act.[102] A court would then likely find an even clearer legislative acknowledgment of the harm that results from a violation of a data breach law like the one in Washington, which includes stronger language than the FCRA to allow an individual to bring a lawsuit for violations of the act.[103]

The failure to learn of a data breach is harmful because hackers will employ an individual's stolen personal information at some point in the future. The question is not if they will do so, but when. As the Seventh Circuit recently explained, there is a reasonable likelihood that hackers will use a plaintiff's information to commit identity theft or credit card fraud,[104] and their criminal motive can be presumed.[105] As Professor Daniel Solove notes, "[w]hy would more than 90% of the states pass data-breach notification laws in the past decade if breaches did not cause harm?"[106] The same is true for the harm that arises from failing to comply with those notification laws. State legislatures included private right of action provisions in these laws to allow individuals to sue a company for failure to comply with their statutory duty to notify them of a breach, and to recover for the harm that occurred as a result. The Supreme Court's holding in *Spokeo* should, therefore, be interpreted to allow individuals to bring suit once their data has been breached, consistent with state legislators' intent in enacting data breach laws with these provisions. Failure to notify impacted individuals of a breach in compliance with state law is injurious in and of itself, and the right to bring suit is necessary to ensure that individuals hold companies accountable in disclosing a breach and allowing them to protect themselves from additional harm. Failure to comply with state data breach laws is meant to be challenged in court when the legislation explicitly includes a private right of action provision.

V. THE SIMILARITIES BETWEEN THE HARM THAT OCCURS FROM A DATA BREACH AND TORT LIABILITY

In the *Lujan* case, Justice Scalia suggested that an injury-in-fact sufficient to confer standing may be found if the alleged injury suffered is

---

102 David N. Anthony & Julie D. Hoffmeister, *FCRA May Be a Dead End for Data Breach Plaintiffs*, LAW360 (Jan. 28, 2016), https://www.law360.com/articles/751612/fcra-may-be-a-dead-end-for-data-breach-plaintiffs.

103 *See An Act Relating to Breaches of Security That Compromise Personal Information*, S.B. 6043, 2005 Leg., Sess. 1, 3 (Wash. 2005).

104 *The Seventh Circuit Sides with Plaintiffs in Data Breach Litigation*, FOX ROTHSCHILD LLP (July 24, 2015), https://dataprivacy.foxrothschild.com/2015/07/articles/data-protection-law-compliance/the-seventh-circuit-sides-with-plaintiffs-in-data-breach-litigation/.

105 Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 779 (2018).

106 Solove, *supra* note 37.

akin to one recognized at common law.[107] Therefore, it could be argued that further evidence of a legislative intent to confer standing for the violation of state data breach laws is the fact that there appears to be a tort-like duty imposed on holders of information that, under the common law, would allow a litigant to obtain standing if breached.

There is evidence of legislative intent to impose a tort-like duty on holders of individuals' sensitive information in that a number of state data breach laws also allow an individual impacted by a violation to bring suit under the state's consumer protection laws.[108] Alaska,[109] Maryland,[110] Tennessee,[111] Texas,[112] and most recently, South Dakota,[113] each have enacted these types of provisions. One of the purposes that states had in enacting these types of consumer protection laws with private rights of action was to help carry out common-law liability since the Federal Trade Commission Act had no such provision.[114] This Act was enacted by Congress in the early twentieth century to provide stronger remedies to consumers who brought claims regarding business torts.[115] Given the law's shortcomings, however, most business torts are now brought under state consumer protection statutes.[116] Therefore, linking the violation of a state data breach law by a business to a private right of action under consumer protection statutes is evidence of a state legislature's intent to treat data breach cases similarly to tort cases.

In fact, the tort-like duty that state data breach laws impose on companies has also been expressed by federal representatives, in addition to state legislators. In recent communications from members of Congress, they have spoken about "hold[ing] Equifax accountable for failing to safeguard our personal information."[117] At the recent hearing held by Congress, Representative Greg Walden of Oregon told the former CEO of Equifax that

---

107 Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

108 *Data Breach Charts*, BAKERHOSTETLER (July 2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/DataBreachCharts.pdf.

109 ALASKA STAT. § 45.48.010 (2015).

110 MD. CODE ANN., COM. LAW § 14-3504 (West 2010).

111 TENN. CODE ANN. §47-18-2107 (2005).

112 TEX. BUS. & COM. CODE § 521.053 (West 2009).

113 *South Dakota Enacts Breach Notification Law*, HUNTON ANDREWS KURTH LLP: PRIVACY & INFORMATION SECURITY L. BLOG (Mar. 23, 2018), https://www.huntonprivacyblog.com/2018/03/23/south-dakota-enacts-breach-notification-law/.

114 Michael C. Gilleran, *The Rise of Unfair and Deceptive Trade Practice Act Claims*, A.B.A. (Oct. 17, 2011), http://apps.americanbar.org/litigation/committees/businesstorts/articles/fall2011-unfair-deceptive-trade-practice-act-claims.html.

115 *Id.*

116 *Id.*

117 What You Should Know About Equifax Data Breach, *supra* note 93.

the company's failure to protect individuals' data from being hacked, and its delay in notifying individuals after it occurred, was "like the guards at Fort Knox forgot to lock the doors and failed to notice the thieves were emptying the vaults."[118]

Plaintiffs often bring negligence claims when suing a company after a data breach occurs, and courts have found those claims viable at the motion to dismiss phase when connected to the violation of a state consumer protection statute. The aftermath of the Target data breach provides a recent example of a court imposing a duty on a company that retains consumer information.[119] In a case that was filed after that breach, the United States District Court for the District of Minnesota concluded that the consumers' allegations that Target knew that the data was sensitive, and therefore was susceptible to being hacked, was plausible enough to establish a duty on Target to disclose the incident.[120] As a result of this finding, most of the class members' claims under state consumer protection laws were sustained in that case.[121] "[T]he existence of the MPSCA bolstered [the] ruling that the financial institutions adequately pleaded a duty of care under general negligence law . . . ."[122] This was because the court felt that the statute stood for "Minnesota's policy of punishing companies that do not secure consumers' credit- and debit-card information."[123] In addition, recently, two Oregon residents filed a class action suit against Equifax, claiming that the company negligently failed to protect their personal information or to use adequate safeguards to protect consumers' personal information.[124] Given the magnitude of the Equifax breach, and the continuing occurrence of other data breaches, courts are likely to see similar cases filed on the basis of tort-related theories.

Recent federal court decisions have also identified the close relationship between harm that is suffered by failure to comply with data breach laws and torts. In the case of *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit held that "Congress has long provided plaintiffs

---

118 Puzzanghera, *supra* note 94.

119 Maggie Lassack, Wendell Bartnick & Joseph Molosky, *Consumer and Financial Instutition Class Actions Survive Motions to Dismiss in Target Data Breach Litigation*, WILSON SONSINI GOODRICH & ROSATI (Feb. 15, 2015), http://www.wsgrdataadvisor.com/2015/02/consumer-and-financial-institution-class-actions-survive-motions-to-dismiss-in-target-data-breach-litigation/#_ftnref5.

120 *Id*.

121 *Id*.

122 Lassack, Wendell & Molosky, *supra* note 119.

123 *Id.*

124 Maxine Bernstein, *Two Oregon Residents File Class Action Lawsuit Against Equifax, Alleging Negligence*, OREGONIAN (Sept. 8, 2017), http://www.oregonlive.com/portland/index.ssf/2017/09/two_oregon_residents_file_clas.html.

with the right to seek redress for unauthorized disclosure of information that, in Congress's judgment, ought to remain private."[125] Further, finding standing based on an alleged violation of the FCRA, in the recent case of *Perrill v. Equifax Information Services, LLC*, the United States District Court for the Western District of Texas stated that "[t]he common law has long recognized a right to personal privacy."[126] Given this reasoning, one could conclude that failure to comply with data breach laws is akin to the tort of public disclosure of private facts, which allows individuals to sue for the unauthorized release of their private information.

Justice Scalia's opinion in *Lujan* did note that statutes cannot create standing in certain circumstances, where the new legal right was not one that was recognized at common law.[127] He was careful, however, to note that the decision was not based on a case where concrete injury had been suffered by many persons, as in mass fraud or mass tort situations.[128] Arguably, then, Justice Scalia's reasoning in *Lujan*, while discrediting private right of action provisions that are too attenuated from actual injury, actually supports the notion that these provisions in state data breach laws should confer standing. This is because the injury in data breach scenarios, as in mass torts, is often suffered by many persons. Even in the *Spokeo* case, which also failed to confer standing based on a private right of action provision, Justice Thomas's concurrence noted the difference between a statute that creates a private right of action based simply on a violation of private rights, versus those that the defendant owed to the public collectively.[129] Given the pervasive nature of data breaches and their impact on society at large, it would be hard to deny that not only do information holders owe a duty to the individuals whose information they possess, but also to the public at large to safeguard the information that they hold to prevent data hacking. An entity that fails to protect the data of many individuals violates the duty of reasonable care that it owes to customers and to members of the public, and therefore, even under the strict *Spokeo* test for standing, a plaintiff who sues a company after experiencing a data breach claims an "intangible harm [that] has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit."[130] That harm is most akin to tort liability.

---

125 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 274 (3d Cir. 2016).

126 Perrill v. Equifax Info. Servs., LLC, 205 F. Supp. 3d 869, 873 (W.D. Tex. 2016) (quoting Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641, 646 (N.D. W. Va. 2016)).

127 Lujan v. Defs. of Wildlife, 504 U.S. 555, 572 (1992).

128 *Id.*

129 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (Thomas, J., concurring).

130 *Id.* at 1549.

Finally, Justice Kennedy's concurrence in *Lujan* provides additional support for state statutory standing provisions in data breach notification laws. Justice Kennedy noted that in creating private rights of action via statute, the legislature "must at the very least identify the injury it seeks to vindicate and relate the injury to the class of persons entitled to bring suit."[131] In most data breach laws with private right of action provisions, only those "injured" by a violation of the statute can bring suit.[132] Therefore, those legislatures have adequately related the class of persons entitled to bring suit by ensuring that only those whose data was compromised, or only those who the data holder breached their duty to, can challenge the violation of that statute.

These cases and decisions reinforce the view that the risk of data breaches imposes tort-like liability on entities that maintain personally identifiable information for consumers, and that state legislators recognized the harm and injury that can occur for failure to comply with a data breach law when drafting private rights of action.

VI. THE CURRENT SPLIT POST-*SPOKEO* REGARDING WHETHER STATE LAW PRIVATE RIGHT OF ACTION PROVISIONS CAN CONFER ARTICLE III STANDING, AND WHY THE ISSUE SHOULD BE RESOLVED IN FAVOR OF UPHOLDING STATUTORY STANDING IN THE DATA BREACH CONTEXT

Since the *Spokeo* decision in 2016, a number of federal court decisions have addressed whether state statutory private rights of action can confer standing.[133] This issue has resulted in a circuit split in which some courts have found standing based on the violation of a state law after a data breach occurred, and some have not.[134] Even before the Court decided *Spokeo*, the Ninth Circuit in 2001 reasoned that "the violation of a state-created legal right . . . can create interests that support standing in federal courts."[135] The court noted that, practically, without conferring standing in this scenario, "there would not be Article III standing in most diversity cases, including run-of-the-mill contract and property disputes."[136] There is also well-established historical support for conferring standing when a plaintiff alleges the violation of a state statute. In the 1988 case of *FMC Corp. v. Boesky*, the Seventh Circuit considered the question of whether the "invasion of a

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

132 *See supra* note 104 and accompanying text.

133 Ronnie Solomon, *Post-Spokeo, Standing Challenges Remain Unpredictable*, LAW360 (Oct. 26, 2016), https://www.law360.com/articles/854898/post-spokeo-standing-challenges-remain-unpredictable.

134 *Id.*

135 Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001).

136 *Id.*

recognized state-law right in itself satisf[ies] Article III's injury requirement, even though an injury separate and apart from the actual invasion is difficult to identify."[137] Though they declined to answer the question directly, the judges cited to a 1975 Supreme Court case in which the Justices explained that "actual or threatened injury required by Art[icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[138]

Even in light of this past practice, however, certain federal courts have unnecessarily denied litigants standing based upon their claim that a state data breach law was violated. In the case of *Khan v. Children's National Health System*, the Fourth Circuit recently held that individuals who brought a class action lawsuit after a data breach occurred did not have standing under the *Spokeo* standard.[139] The court reasoned that "[h]ere, where Khan alleges violations of state law, she advances no authority for the proposition that a state legislature or court, through a state statute or cause of action, can manufacture Article III standing for a litigant who has not suffered a concrete injury."[140] The Ninth Circuit, however, consistent with the position that it took in the 2001 case of *Cantrell v. City of Long Beach*,[141] has continued to provide that "state statutes can create interests that support standing in federal courts," even post-*Spokeo*.[142] In the 2016 case of *Matera v. Google*, the United States District Court for the Northern District of California interpreted the *Spokeo* decision as setting forth three factors that "grant . . . persons in the plaintiff's position a right to judicial relief."[143] Those factors are: "(1) the *provision of a private right of action*; (2) the availability of statutory damages; and (3) the substantive nature of the statutory right."[144] In *Matera*, the court upheld the plaintiff's right to sue Google based on the violation of the California Invasion of Privacy Act.[145] Clearly, then, at least some federal courts understand the *Spokeo* decision as having validated the ability of state statutes to confer standing to litigants in federal court who allege the violation of the law; an ability that existed long before the Supreme Court decided the *Spokeo* case. This lends credence to the argument that individuals should be permitted to bring a case against companies who failed to comply with data breach notification laws when those laws establish a

137 FMC Corp. v. Boesky, 852 F.2d 981, 993 (7th Cir. 1988).

138 Warth v. Seldin, 422 U.S. 490, 500 (1975) (internal quotations omitted).

139 Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524 (D. Md. 2016).

140 *Id.* at 534.

141 241 F.3d 674, 684 (9th Cir. 2001).

142 Matera v. Google, Inc., No. 15-cv-04062, 2016 WL 5339806, at *14, n.2 (N.D. Cal. Sept. 23, 2016).

143 *Id.*

144 *Id.* (emphasis added).

145 *Id.*

private right of action.

In addition to the Ninth Circuit, federal judges in the Southern District of New York have recently granted standing to plaintiffs claiming the violation of a state mortgage-notification statute.[146] In the 2016 case of *Bellino v. JP Morgan Chase*, the court reasoned that "[u]ltimately, both history and the judgment of the New York State legislature indicate an intent to elevate the harm associated with a mortgagee's delayed filing . . . to a concrete injury."[147] In addition, in the recent case of *Jaffe v. Bank of America*, which also analyzed standing for the violation of the mortgage notification law, the Southern District of New York held that "[t]he State Legislature has provided a private right of action and a heuristic for quantifying damages, possibly in recognition of [] the concreteness of this harm."[148] The *Jaffe* court further stated that "[t]he types of harm the statutes protect against are real."[149] In both *Bellino* and *Jaffe*, the courts evaluated a claim of failure to comply with state law that requires banks to file timely mortgage satisfaction information, and both found that the legislature intended this failure to be a harm that could be remedied in court.[150] This scenario is strikingly similar to the data breach context, where failure to timely notify an individual of a breach of their data can cause real, concrete harm. In addition, a number of other recent federal court decisions have upheld standing for the alleged violation of privacy and data security laws, including *Boelter v. Advance Magazine Publishers*, where the court found that the failure to comply with the Michigan Preservation of Personal Privacy Act was sufficient to allow the case to proceed.[151]

Long before *Spokeo*, federal courts recognized state legislatures' ability to confer standing to plaintiffs who allege the violation of a law which allows them to bring suit,[152] and after *Spokeo*, many federal courts continue to allow parties to claim the violation of a state law with a private right of action provision in order to allege injury-in-fact sufficient to obtain standing.[153] Consistent with the Ninth Circuit's reasoning[154] and recent decisions made by judges in the Southern District of New York,[155] the current circuit split

146 Bellino v. JPMorgan Chase Bank, N.A., 209 F. Supp. 3d 601 (S.D.N.Y. 2016); Jaffe v. Bank of Am., N.A., 197 F. Supp. 3d 523 (S.D.N.Y. 2016).

147 *Bellino*, 209 F. Supp. 3d at 610.

148 *Jaffe*, 197 F. Supp. 3d at 528.

149 *Id.*

150 *See Bellino*, 209 F. Supp. 3d at 601; *see also Jaffe*, 197 F. Supp. 3d at 523.

151 Boelter v. Advance Magazine Publishers, Inc., 210 F. Supp. 3d 579 (S.D.N.Y. 2016).

152 *See* Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001).

153 *See, e.g.*, Matera v. Google, Inc., No. 15-cv-04062, 2016 WL 5339806, at *14, n.2 (N.D. Cal. Sept. 23, 2016).

154 *Id.*

155 *See Bellino*, 209 F. Supp. 3d at 601; *see also Jaffe*, 197 F. Supp. 3d at 523.

should be resolved in favor of understanding the *Spokeo* decision as having affirmed the right of state legislatures to confer standing via their statutes, and not as barring their ability to do so.

VII. CONCLUSION

The question of whether private right of action provisions in state data breach laws confer standing to plaintiffs whose information has been acquired may not be resolved definitively in the near future, as a number of laws allow individuals "injured" under the statute to file suit,[156] which may create ambiguity. Therefore, federal courts may continue to assess on a case-by-case basis whether class members were sufficiently harmed by the violation of the statute, such that Article III injury-in-fact was attained. If a lawsuit based on a state data breach law was heard by the Supreme Court and remanded to determine injury, as the *Spokeo* case was remanded to the Ninth Circuit who found sufficient injury,[157] however, the decisions on remand about whether the risk of harm experienced by those impacted by a data breach is injurious enough to confer standing may provide guidance to future litigants.[158] In addition, in the Seventh Circuit, the recent holding in *Remijas v. Neiman Marcus Group, LLC* may allow individuals who have suffered a breach of their data to bring a claim based solely on the violation of a state data breach law, because the court found that the future risk of theft and fraud suffices for standing purposes.[159] Adding to the uncertainty is the fact that "*Spokeo* only sets limits on federal-court jurisdiction; state-court jurisdiction is not limited by Article III."[160] "Thus, a case dismissed from federal court under *Spokeo* could be re-filed in state court, although some (but not all) state courts find federal Article III cases instructive when interpreting limits on state-court subject-matter jurisdiction."[161]

Nonetheless, in light of the way that harm occurs after a data breach, the purpose of private right of action provisions, and the tort-like duty imposed on entities that hold individuals' personal data, it is clear that state legislators intended for individuals affected by a data breach to be able to bring suit when they drafted these laws. Therefore, the *Spokeo* decision should not bar class action suits alleging the violation of a state data breach law that includes a private right of action, if such a violation occurs and individuals are not timely warned of the acquisition of their personal, sensitive information.

156 *See* CAL. CIV. CODE § 1798.84(b) (West 2010).
157 Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).
158 *Id.*
159 Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015).
160 Fleischmann, Perdew & Shetty, *supra* note 33.
161 *Id.*