Utah Law Review

Volume 2019 | Number 3 Article 6

6-2019

The Path to Standing: Asserting the Inherent Injury of the Data Breach

Jennifer M. Joslin
S.J. Quinney College of Law, University of Utah

THE PATH TO STANDING: ASSERTING THE INHERENT INJURY OF THE DATA BREACH

Jennifer M. Joslin*

Abstract

Data breaches are on the rise as consumers continue to exchange personally identifiable information for goods and services in sectors from retail to healthcare. In the aftermath of a data breach, it has been difficult for victims of the breach to establish Article III standing to sue in federal courts. The primary hurdle for those seeking a remedy for the theft of their data has been showing that they have suffered an injury-in-fact. Plaintiffs typically assert an injury based on the increased risk of identity theft following a breach. However, courts have divided on whether such an injury satisfies the standing test. For consumers who feel deeply that they have been harmed, a court's aversion to increased-risk standing is a devastating barrier to redress.

This Note argues that courts should consider a different point of injury. Rather than looking at the risk of future identity theft, courts should analyze standing based on the injury that consumers suffer the moment their data is stolen. Looking to the Supreme Court's decisions in Clapper v. Amnesty International USA *and* Spokeo, Inc. v. Robins, *this Note argues that the inherent injury of the data breach is an actual, concrete, and particularized injury that is sufficient to confer standing.*

Ultimately, shifting the standing inquiry to the inherent injury of the data breach will ensure that meritorious claims are heard in court. The shift is easily implemented—it comports with existing precedent, requires no new action by Congress or the Supreme Court, and is harmonious with the principles that underlie the doctrine of standing. Most importantly, the shift will ensure access to justice for a growing body of consumers who have been harmed by a data breach.

INTRODUCTION

As society becomes increasingly digitized, the private information of everyday consumers becomes increasingly exposed to bad actors. With every hospital visit, credit card application, or subscription to the latest meal-kit service, consumers are compelled to exchange their personal information for goods and services. Unfortunately, with cyberattacks and institutional data breaches on the rise, consumers are increasingly likely to find their private information in the hands—or

 J.D. Candidate 2019 at the University of Utah, S.J. Quinney College of Law. Special thanks to the *Utah Law Review* and Professor Lincoln Davies. Immense gratitude to my friends and family—especially my parents.

on the screens—of bad actors.[1] In 2017, hackers executed 1,579 data breaches in the United States, a 44.7 percent increase from 2016.[2] Those 1,579 data breaches exposed over 178 million records.[3] In November 2018, a massive breach of Marriott International's Starwood hotel system exposed over 500 million records,[4] continuing a vicious uptick in the data-theft trend.

In the aftermath of an institutional data breach, consumers are left wondering where and from whom they can seek redress. Just as critically, as data breach victims turn to litigation to seek a remedy for the theft of their personal information, they sometimes face constitutional barriers to presenting their case. When data breach plaintiffs bring claims in federal court, they—like any other plaintiff—must establish that they have standing to sue under Article III of the U.S. Constitution before they can even attempt to prove their claims on the merits.[5] To establish standing, plaintiffs must show they have satisfied the now well-known three-part test: they must assert (1) an injury-in-fact that is both (2) fairly traceable to the challenged action and (3) redressable by a favorable judicial decision.[6] For data-breach plaintiffs, properly alleging an injury-in-fact has typically been the greatest hurdle to establishing standing.

Over the last decade, data-breach plaintiffs generally have sought to show an injury-in-fact by alleging an injury based on an increased risk of identity theft.[7] Courts have divided on whether such an injury satisfies the standing test. The U.S. Court of Appeals for the Sixth,[8] Seventh,[9] and Ninth Circuits[10] have embraced this

---

[1] *At Mid-Year, U.S. Data Breaches Increase at Record Pace*, PR NEWSWIRE (July 18, 2017, 8:00 AM), https://www.prnewswire.com/news-releases/at-mid-year-us-data-breaches-increase-at-record-pace-300489369.html [https://perma.cc/5MYD-G6WW].

[2] IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 3 (2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf [https://perma.cc/BC7Y-UXH7].

[3] *Id.* at 6.

[4] IDENTITY THEFT RES. CTR., MONTHLY BREACH REPORT: NOVEMBER 2018, at 2 (Dec. 5, 2018), https://www.idtheftcenter.org/wp-content/uploads/2018/12/2018-November-Monthly-Breach-List.pdf [https://perma.cc/7S5A-2BRY].

[5] Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 102 (1998) (explaining that every court must answer the "threshold jurisdictional question" of whether the plaintiff has "standing to sue" under Article III of the U.S. Constitution).

[6] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

[7] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632–33 (7th Cir. 2007) (alleging an increased risk of identity theft following the breach of a banking website); Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) (alleging an increased risk of identity theft after two data breaches at a medical center).

[8] *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 392 (6th Cir. 2016) (granting increased-risk standing).

[9] *See Pisciotta,* 499 F.3d at 634 (granting increased-risk standing); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015) (granting increased-risk standing).

[10] *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (granting increased-risk standing).

increased-risk theory as a cognizable injury. But the First,[11] Third,[12] Fourth,[13] and Eighth[14] Circuits have declined to recognize increased-risk standing in data breach cases. Two recent Supreme Court decisions have only further clouded the issue: *Clapper v. Amnesty International USA*,[15] and *Spokeo, Inc. v. Robins*.[16] Indeed, lower courts have applied *Clapper* and *Spokeo* to reach different results on the standing question for data-breach victims.[17] For data-breach victims seeking redress in the courts, this divergence in case law runs contrary to the principles of justice, efficiency, and predictability that underlie the federal judiciary.

In light of this uncertainty, scholars have proposed a number of solutions. These proposals include factor-based frameworks to determine when an increased risk of identity theft may qualify as an injury-in-fact[18] and statutory solutions that provide a right to data security.[19] Some commentators have suggested that courts have applied *Clapper*[20] and *Spokeo* incorrectly. Others have argued that existing standards for unauthorized government surveillance should be applied to data-breach cases.[21] However, these arguments are hindered by congressional inefficiency and the Supreme Court's reluctance to rule definitively on the standing question for data breach plaintiffs. Considering the dramatic rise of data breaches in the United States, coupled with the absence of congressional or Supreme Court guidance in the context of data breach litigation, it would be prudent for courts to adopt an approach that is

---

[11] *See* Katz v. Pershing, LLC, 672 F.3d 64, 78–80 (1st Cir. 2012) (denying increased-risk standing).

[12] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (denying increased-risk standing).

[13] *See* Beck v. McDonald, 848 F.3d 262, 273–76 (4th Cir. 2017) (denying increased-risk standing).

[14] *See In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (denying increased-risk standing).

[15] 568 U.S. 398 (2013).

[16] 136 S. Ct. 1540 (2016).

[17] *See, e.g.*, *Beck*, 848 F.3d at 275 (holding that the increased risk of identity theft was not "certainly impending" under *Clapper*); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015) (finding that the increased risk of identity theft *was* "certainly impending" under *Clapper*).

[18] Thomas Martecchini, Note, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After* Clapper v. Amnesty International USA, 114 MICH. L. REV. 1471, 1493 (2016).

[19] *See generally* Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79 (2017) (arguing that Congress should pass a statute giving data breach victims standing to sue).

[20] Andrew Braunstein, Note, *Standing Up for Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing*, 24 J.L. & POL'Y 93, 98 (2015).

[21] Nick Beatty, Note, *Standing Room Only: Solving the Injury-in-Fact Problem for Data Breach Plaintiffs*, 2016 BYU L. REV. 1289, 1313–15 (2016).

rooted in Supreme Court jurisprudence, does not conflict with existing precedent within the circuits, and would ensure fairness and predictability for future data breach plaintiffs.

This Note endeavors to provide such a solution. First, this Note discusses the doctrine of standing and considers the injury-in-fact requirement through the lens of *Clapper* and *Spokeo*. Next, it examines two cases that each reflect a general—and divergent—approach to increased-risk standing after *Clapper* and *Spokeo*. This Note then argues that courts should analyze an injury based on the theft of personal information *during* the breach, irrespective of any risk of identity theft *following* the breach. Finally, it goes on to analyze the inherent injury of the data breach under existing case law and argues that the theft of personal information during the breach is an injury-in-fact sufficient to confer standing.

I. BACKGROUND

A. The Doctrine of Standing

At the outset of any litigation in federal court,[22] a plaintiff must show that she has standing to sue.[23] In other words, the plaintiff must demonstrate that a federal court has the *power* to adjudicate her case, irrespective of the relative strengths of her claims.[24] The doctrine of standing derives from the Constitution's division of federal governmental powers between the legislative,[25] executive,[26] and judicial[27] branches.[28] Article III of the Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies," but it goes no further to define those terms.[29] Accordingly, the Supreme Court has developed the doctrine of standing to illuminate the parameters of justiciability under Article III and to reinforce the "proper—and properly limited—role of the courts in a democratic society."[30]

To show that she has standing to sue in a federal court, a plaintiff must establish three things: (1) that she has suffered an injury-in-fact, (2) that the injury is fairly traceable to the action of the defendant, and (3) that the injury is redressable by a

---

[22] Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 94–95 (1998) ("The requirement that jurisdiction be established as a threshold matter 'spring[s] from the nature and limits of the judicial power of the United States' and is 'inflexible and without exception.'") (quoting Mansfield, C. & L.M. Ry. Co. v. Swan, 111 U.S. 379, 382 (1884)).

[23] *Id.* at 102.

[24] *Id.* at 89; Bell v. Hood, 327 U.S. 678, 682 (1946) ("Jurisdiction . . . is not defeated . . . by the possibility that the averments might fail to state a cause of action on which petitioners could actually recover.").

[25] U.S. CONST. art. 1, § 1.

[26] *Id.* art. 2, § 1.

[27] *Id.* art. 3, § 1.

[28] Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992).

[29] *Id.*

[30] Warth v. Seldin, 422 U.S. 490, 498 (1975).

favorable judicial decision.[31] In data breach litigation, the most daunting hurdle for plaintiffs typically has been establishing an injury-in-fact. This Note will analyze the injury-in-fact requirement through the lens of two recent cases: *Clapper v. Amnesty International USA*,[32] and *Spokeo, Inc. v. Robins*.[33]

An injury-in-fact is "an invasion of a legally protected interest."[34] The injury must be "actual or imminent" and both "concrete" and "particularized."[35] First, the alleged injury must be either actual—that is, the injury has occurred or is ongoing—or it must be imminent.[36] An imminent injury will only support standing if it is "certainly impending."[37] Next, a concrete injury must be *de facto*; it must actually exist and cannot be merely abstract.[38] Finally, a particularized injury "must affect the plaintiff in a personal and individual way."[39]

1. Actual or Imminent

A properly alleged injury-in-fact must be "actual or imminent, not conjectural or hypothetical."[40] In other words, a plaintiff may assert injury based on harm that has already occurred or is ongoing, or a plaintiff may assert a threatened injury that is "imminent."[41] The Supreme Court has acknowledged that the question of imminence is "a somewhat elastic concept," although its purpose is clear—"to ensure that the alleged injury is not too speculative."[42] Accordingly, "[a]llegations of *possible* future injury" are not sufficient.[43] Rather, an imminent injury will only support standing if it is "certainly impending."[44]

The Supreme Court addressed "imminence" in *Clapper*, wherein the Court faced a constitutional challenge to § 1881a of the Foreign Intelligence Surveillance Act of 1978.[45] That provision permits the Attorney General and the Director of National Intelligence to jointly authorize the surveillance of non-U.S. persons who are reasonably believed to be located outside the United States.[46] The provision was challenged by a group of attorneys and human rights, labor, legal, and media

---

[31] *Lujan*, 504 U.S. at 560–61.

[32] 568 U.S. 398 (2013).

[33] 136 S. Ct. 1540 (2016).

[34] *Lujan*, 504 U.S. at 560.

[35] Monsanto Co. v. Geerston Seed Farms, 561 U.S. 139, 149 (2010).

[36] *Id.*

[37] *Lujan*, 504 U.S. at 565 n.2 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[38] *Spokeo*, 136 S. Ct. at 1548.

[39] *Lujan*, 504 U.S. at 560 n.1.

[40] *Id.* at 560 (quotations and citations omitted).

[41] Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 472 (1982) (citation omitted).

[42] *Lujan*, 504 U.S. at 565 n. 2.

[43] Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (emphasis added).

[44] *Lujan*, 504 U.S. at 565 n.2 (quoting *Whitmore*, 495 U.S. at 158).

[45] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[46] *Id.*

organizations who engage in sensitive communications with non-U.S. persons that would be likely targets of surveillance under § 1881a.[47] The plaintiffs alleged that § 1881a quelled their communications and compelled them to travel abroad to have in-person conversations, rather than speak by telephone or email.[48] After both parties moved for summary judgment, the district court dismissed the case for lack of standing.[49] The Second Circuit reversed on appeal, and the Supreme Court granted certiorari to determine whether the plaintiffs had properly shown an injury-in-fact.[50]

In *Clapper*, the plaintiffs alleged an "imminent" injury, claiming that there was an objectively reasonable likelihood that their communications would be acquired under § 1881a at some point in the future.[51] The court rejected this theory, finding that the respondents failed to assert an injury-in-fact that was "certainly impending."[52] The Court noted that the plaintiffs had no actual knowledge of the Government's surveillance practices under § 1881a and that the plaintiffs were relying on mere assumptions and speculations to support their theory of standing.[53] The Court pointed out that the plaintiffs' theory rested on a "highly speculative fear" that the Government would (1) target persons with whom plaintiffs communicate, (2) invoke its authority under § 1881a, (3) meet the standards imposed by § 1881a and the Fourth Amendment, and (4) succeed in intercepting specific communications to which respondents happened to be a party.[54] The Court duly rejected the plaintiffs' theory of possible future surveillance because it relied on a "highly attenuated chain of possibilities" and required "guesswork as to how independent decisionmakers [would] exercise their judgment."[55] Although there was a possibility of future surveillance, the plaintiffs failed to show that surveillance was "certainly impending."[56] Thus, the alleged injury was neither "actual" nor "imminent."

2. Concrete and Particularized

In addition to showing that the injury is "actual or imminent," plaintiffs must show that the injury is both "concrete" and "particularized."[57] For an injury to be "concrete," it "must be '*de facto*'; that is, it must actually exist."[58] A tangible injury, such as economic or physical harm, is easy to recognize as a concrete injury.[59]

---

[47] *Id.* at 406.
[48] *Id.* at 406–07.
[49] *Id.* at 407.
[50] *Id.*
[51] *Id.*
[52] *Id.* at 414.
[53] *Id.* at 411.
[54] *Id.* at 410.
[55] *Id.* at 410, 413.
[56] *Id.* at 414.
[57] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).
[58] *Id.*
[59] *Id.* at 1549.

However, an intangible harm also may be a "concrete" injury when it "has a close relationship to a harm that has traditionally . . . provid[ed] a basis for a lawsuit in English or American courts"[60] or when Congress has manifested an intent to "elevat[e]" the intangible harm "to the status of [a] legally cognizable injur[y]."[61] For an injury to be "particularized," it "must affect the plaintiff in a personal and individual way."[62]

In *Spokeo*, the Supreme Court addressed principles of concreteness and particularization for an aggrieved consumer who sued Spokeo, Inc. ("Spokeo").[63] Spokeo is the operator of a "people search engine" that provides information such as a person's address, marital and employment status, and education.[64] After discovering that his Spokeo profile contained wildly inaccurate information, the plaintiff filed a class-action complaint, claiming that Spokeo had willfully violated provisions of the Fair Credit Reporting Act of 1970 ("FCRA"), including the requirement to engage in "fair and accurate credit reporting."[65] The district court dismissed the case for lack of standing, finding that the plaintiff had not properly pled an injury-in-fact.[66] The Ninth Circuit reversed on appeal, and the Supreme Court granted certiorari, taking the opportunity to expound on the requirements for showing an injury-in-fact.[67]

In *Spokeo*, the plaintiff alleged an injury-in-fact based on violations of his statutory rights under the FCRA.[68] The Court conducted its analysis with an eye toward concreteness and particularization, making clear from the outset that both elements are necessary, but neither is sufficient, to establish an injury-in-fact.[69] The Court noted that the Ninth Circuit had properly addressed the particularization element.[70] The Ninth Circuit concluded that the plaintiff's injury affected him in a "personal and individual way" because he was alleging the violation of *his* statutory rights, not just the rights of other people.[71] The Ninth Circuit found additional support for particularization because the plaintiff's personal interests in the handling of his credit information were "individualized rather than collective."[72] The Supreme Court found, however, that the Ninth Circuit had failed to determine whether the alleged injury was concrete in addition to being particularized.[73] The Court

---

[60] *Id.*
[61] *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)).
[62] *Lujan*, 504 U.S. at 560 n.1.
[63] *Spokeo*, 136 S. Ct. at 1546.
[64] *Id.*
[65] *Id.* at 1545–46 (citations omitted).
[66] *Id.* at 1546.
[67] *Id.* at 1546, 1547–50.
[68] *Id.* at 1546.
[69] *Id.* at 1548.
[70] *Id.*
[71] *Id.*
[72] *Id.* (citation omitted).
[73] *Id.* at 1550.

ultimately remanded the case to the Ninth Circuit for a factual determination, but not before addressing the basic principles of concreteness.[74]

A concrete injury must be *de facto*.[75] In other words, it must actually exist; it must be real and not abstract.[76] The Court was careful to note, however, that "concrete" is not necessarily synonymous with "tangible."[77] Indeed, courts have traditionally upheld standing in the absence of physical or financial harm for torts such as trespass and defamation,[78] and courts have even recognized intangible injuries to spiritual and aesthetic interests.[79] In determining whether an intangible harm is a concrete injury-in-fact, the Court proclaimed that "both history and the judgment of Congress play important roles."[80] The Court recalled that the standing doctrine's "case or controversy" requirement is rooted in historical practice.[81] Accordingly, "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."[82] The Court also pointed to the judgment of Congress, noting that "Congress is well positioned to identify intangible harms that meet minimum Article III requirements."[83] However, the Court cautioned that a plaintiff could not satisfy the injury-in-fact requirement by alleging a "bare procedural [statutory] violation" in the absence of any concrete harm.[84] Finally, the Court cited to *Clapper*, confirming that the risk of real harm may be concrete when the risk is "imminent."[85]

B. Competing Applications of Clapper *and* Spokeo

Over the last decade, courts have divided regarding Article III standing for data breach plaintiffs.[86] In these cases, plaintiffs have generally attempted to establish standing based on the increased risk of identity theft following the breach.[87] In the wake of *Clapper* and *Spokeo*, courts have reached different conclusions about

---

[74] *Id.* at 1548–50.

[75] *Id.* at 1548.

[76] *Id.*

[77] *Id.* at 1549.

[78] Beatty, *supra* note 21, at 1295.

[79] Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1377 (2013).

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

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (granting standing for data breach plaintiffs); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing for data breach plaintiffs).

[87] *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased risk of identity theft was sufficient to confer standing).

whether such an injury satisfies the standing test.[88] In general, these holdings have been largely fact-dependent, turning on the type of data that was stolen[89] or whether the data was targeted and understood by hackers.[90] These decisions, however, are representative of a broad willingness or reluctance to recognize increased-risk standing, and they are instructive in analyzing the trajectory of data breach standing.

This Note will address two cases that each reflect a general approach to increased-risk standing for data breach plaintiffs. First, in *Galaria v. Nationwide Mutual Insurance Company*,[91] the Sixth Circuit granted standing based on the increased risk of identity theft. Next, in *Alleruzzo v. SuperValue, Inc.*,[92] the Eighth Circuit declined to recognize increased-risk standing.

1. Approach One: Recognizing Increased-Risk Standing

In *Galaria*, the Sixth Circuit determined that data breach plaintiffs had Article III standing to sue based on the increased risk of identity theft following the breach.[93] In 2012, hackers broke into the computer network at Nationwide Mutual Insurance Company ("Nationwide"), stealing the personally identifiable information ("PII") of over one million individuals.[94] The stolen data included names, birthdates, genders, occupations, driver's license numbers, and social security numbers.[95] Following the breach, a class of individuals whose PII was stolen sued Nationwide.[96] The plaintiffs brought claims for common-law negligence, invasion of privacy, and willful and negligent violation of the FCRA.[97] The district court dismissed the case for lack of standing, and the plaintiffs appealed.[98]

---

[88] *Compare* Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017) (denying standing based on the increased risk of identity theft arising out of two data breaches at a hospital, noting that the threat of identity theft was based on a "highly attenuated chain of possibilities" (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013))), *with* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) (granting standing after a data breach based on the increased risk of identity theft, noting that "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities").

[89] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (rejecting increased-risk standing for a class of plaintiffs whose credit and debit card information was stolen, but who's personal identifying information was not stolen).

[90] *See, e.g.*, *Beck*, 848 F.3d at 275 (declining to assume that the thieves targeted the stolen laptops for the personal information they contained); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (rejecting increased-risk standing after a hacker penetrated a payroll system firewall because it was "not known whether the hacker read, copied, or understood" the system's information).

[91] 663 F. App'x 384 (6th Cir. 2016).

[92] 870 F.3d 763 (8th Cir. 2017).

[93] *Galaria*, 663 F. App'x at 385.

[94] *Id.* at 386.

[95] *Id.*

[96] *Id.* at 385.

[97] *Id.*

[98] *Id.*

The Sixth Circuit turned to the standing analysis set forth in *Clapper* and *Spokeo* to determine whether the plaintiffs had properly established an injury-in-fact.[99] The court first identified the alleged injury: that the theft of the plaintiffs' PII placed them at a "continuing, increased risk of fraud and identity theft."[100] Because the plaintiffs had alleged an "imminent," rather than an "actual" injury, the court next examined whether the injury was "certainly impending."[101] The court found that the plaintiffs' alleged injury rose beyond the highly "speculative" allegations in *Clapper*.[102] Indeed, the court declared that "[t]here is no need for speculation where Plaintiffs allege that their data *has already been stolen* and is now in the hands of ill-intentioned criminals."[103] Here, the court did not intimate that the theft itself represented an injury-in-fact; however, the court did acknowledge that following the theft of the plaintiffs' PII, "a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."[104] Thus, the court found that the fraudulent misuse of plaintiffs' PII was sufficiently imminent.[105] In so doing, the Sixth Circuit held that the increased risk of identity theft following a data breach is an injury-in-fact sufficient to support standing.[106]

2. Approach Two: Rejecting Increased-Risk Standing

In *SuperValu*, the Eighth Circuit rejected increased-risk standing for a class of plaintiffs following two data breaches at a chain of grocery stores.[107] In August 2014, SuperValu notified its customers that its computer network had been breached by hackers.[108] One month later, SuperValu notified its customers of a second breach.[109] By placing malicious software on SuperValu's network, the hackers had gained access to customers' payment card information ("Card Information"), including names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs).[110] Following the breaches, sixteen SuperValu customers brought suit against the retailer, alleging

---

[99] *Id.* at 387–90. The court also examined whether the injury was fairly traceable to the challenged action and whether the injury was redressable by a favorable decision. *Id.* at 390–91.

[100] *Id.* at 388.

[101] *Id.* (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013)).

[102] *Id.*

[103] *Id.* (emphasis added).

[104] *Id.*

[105] *Id.*

[106] *Id.* at 389. The court also noted that but for Nationwide's allegedly lax data security, the hackers would not have been able to steal the plaintiffs' data. Thus, the injury was fairly traceable to Nationwide's conduct. *Id.* at 390. Additionally, because the plaintiffs sought compensatory damages a favorable decision would provide redress. *Id.* at 391.

[107] *In re* SuperValu, Inc., 870 F.3d 763, 765 (8th Cir. 2017).

[108] *Id.* at 766.

[109] *Id.*

[110] *Id.*

common-law negligence, breach of implied contract, and unjust enrichment.[111] The district court dismissed the claims for lack of standing, and plaintiffs appealed.[112]

The Eighth Circuit first reviewed basic principles of standing, emphasizing that a class action may proceed as long as one named plaintiff has standing.[113] The court then noted that the plaintiffs alleged two theories of standing: (1) the class of plaintiffs alleged an "imminent" injury, arguing that the theft of their Card Information put them at risk of future identify theft, and (2) one named plaintiff alleged an "actual" injury based on a fraudulent charge on his credit card.[114] Turning first to the "imminent" injury, the court recognized that a future injury may support standing when it is "certainly impending."[115] The court found that although the plaintiffs had sufficiently alleged that their Card Information was stolen, they failed to show that any misuse of their Card Information was "certainly impending."[116] Although the court declined to definitively determine whether evidence of misuse following a data breach is necessary to establish standing, the court determined here that the plaintiffs' increased-risk theory failed to support standing.[117]

The court turned next to the "actual" injury alleged by one of the named plaintiffs.[118] The plaintiff alleged that he suffered a fraudulent charge on the credit card he had used to purchase goods at a SuperValu store.[119] The court determined that the misuse of the plaintiff's card information was credit fraud and was thus a form of identity theft.[120] Because identity theft is an actual, concrete, and particularized injury, the court determined that the plaintiff had properly alleged an injury-in-fact sufficient to support standing.[121] What's more, because a class action may proceed if at least one named plaintiff has standing, the court determined the entire class had Article III standing to sue in light of one named plaintiff's "actual" injury.[122]

Although the outcome in *SuperValu* was favorable for the data breach plaintiffs, the court's reasoning in its standing analysis is representative of a broad reluctance to grant standing based on an increased risk of identity theft.

II. ANALYSIS

The division regarding increased-risk standing has caused confusion and unpredictability for data breach plaintiffs. In order to ensure justice, courts should

---

[111] *Id.* at 767.
[112] *Id.*
[113] *Id.* at 768 (citing Horne v. Flores, 557 U.S. 433, 446 (2009)).
[114] *Id.*
[115] *Id.* at 769.
[116] *Id.*
[117] *Id.* at 771–72.
[118] *Id.* at 772.
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.* at 772–74.

adopt an approach that comports with the doctrine of standing and provides access to the judicial system for data breach plaintiffs. This Note makes two arguments to support such an approach. First, courts should shift the injury-in-fact inquiry to the theft of personal information *during* the breach, rather than the increased risk of identity theft *following* the breach. Next, courts should grant standing based on the inherent injury of the data breach in accordance with existing Supreme Court jurisprudence and in line with the principles that underlie the doctrine of standing.

A. Courts Should Shift the Injury-In-Fact Inquiry to the Inherent Injury of the Data Breach

The first step in determining whether a plaintiff has properly established Article III standing is to identify the alleged injury. Only then can the court examine whether the alleged injury is fairly traceable to the challenged action and redressable by a favorable judicial decision.[123] The most common alleged injury in data breach cases is the increased risk of identity theft following the breach.[124] This Note argues that the increased-risk theory, however, is an ineffective means by which to determine whether data breach plaintiffs may be heard in a federal court. Instead, this Note asserts that courts should analyze the elements of standing based on an earlier point of injury: the data breach itself. Specifically, courts should identify and analyze the injury based on the theft of plaintiffs' data and should then determine whether that "actual" injury is "concrete" and "particularized."[125]

Although a court's standing analysis is largely guided by the plaintiff's assertions at the pleading stage, a plaintiff would not need to assert the inherent injury theory in her complaint.[126] Indeed, the Supreme Court has specified that "it is unnecessary to set out a legal theory for the plaintiff's claim for relief" in a pleading.[127] As long as the plaintiff alleges facts demonstrating her actual injury, she has met her burden at the pleading stage.[128] Thus, as long as a plaintiff alleges that her personal information was stolen in a data breach, a court has the power to determine whether the breach itself is an injury-in-fact sufficient to confer standing.

---

[123] Monsanto Co. v. Geerston Seed Farm, 561 U.S. 139, 149 (2010).

[124] *See, e.g.*, Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (alleging increased-risk standing); *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017) (alleging increased-risk standing); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) (alleging increased-risk standing); Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015) (alleging increased-risk standing); Katz v. Pershing, LLC 672 F.3d 64 (1st Cir. 2012) (alleging increased-risk standing); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (alleging increased-risk standing); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (alleging increased-risk standing); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (alleging increased-risk standing).

[125] *Monsanto*, 561 U.S. at 149.

[126] *See SuperValu*, 870 F.3d at 772 (accepting a successful theory of injury despite the plaintiff's failure to plead that theory of injury in the Complaint).

[127] Johnson v. City of Shelby, 135 S. Ct. 346, 347 (2014) (citation omitted).

[128] *SuperValu*, 870 F.3d at 772.

Support for identifying the injury as the breach itself is best shown by analogy to *Clapper*. In *Clapper*, the plaintiffs sought a declaration that a law permitting surveillance of non-U.S. citizens located abroad was unconstitutional.[129] The plaintiffs, believing that their own communications with non-U.S. persons located abroad were likely to be surveilled, sued in federal court.[130] The plaintiffs attempted to establish standing based on a theory of "imminent" injury, asserting an "objectively reasonable likelihood" that their communications would be surveilled under the law in question.[131] Importantly, the plaintiffs could not establish and did not assert that any of their communications had already been targeted.[132]

In contrast, data breach plaintiffs have historically been able to prove the actual theft of their data.[133] Moreover, the existence of the breach has traditionally gone undisputed.[134] Unlike the *Clapper* plaintiffs, who could not prove that they had been subject to surveillance, data breach plaintiffs have proved without contest that they have been subject to lost data.[135] If consumers brought suit against an institution for the negligent stewardship of their data *before* any data breach had occurred, it would be appropriate to apply *Clapper's* imminence analysis and determine whether a data breach was "certainly impending." But where the plaintiff has demonstrated that her data has already been stolen, it would be more appropriate to determine whether that "actual" injury is "concrete" and "particularized" under *Spokeo*.

In recent years, some commentators have advocated for maintaining the theory of increased-risk standing.[136] These arguments propose that courts should recognize increased-risk standing when certain factors are present that elevate the risk to an "imminent" injury in line with *Clapper*.[137] Specifically, these arguments suggest that the increased risk of identity theft is sufficiently imminent when plaintiffs can show that the hack was deliberate and targeted or that there has been fraudulent activity following the breach.[138] Alternatively, some commentators suggest that courts should recognize the increased-risk theory even in the absence of aggravating

---

[129] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 406–07 (2013).

[130] *Id.* at 401.

[131] *Id.* at 407.

[132] *Id.* at 411 ("[R]espondents have no actual knowledge of the Government's § 1881a targeting practices. Instead, respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under § 1881a.").

[133] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals.").

[134] *See id.* at 386 ("On October 3, 2012 hackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others."). Plaintiffs are generally informed that their data has been stolen by the institution that was breached. *See id.*

[135] Braunstein, *supra* note 20, at 108 (arguing that courts have misapplied *Clapper* to data breach cases).

[136] *See* Galbraith, *supra* note 79, at 1371–72; Martecchini, *supra* note 18, at 1474.

[137] Martecchini, *supra* note 18, at 1487.

[138] *Id.*

factors.[139] These arguments analogize to the "latent harm" analysis used in medical malpractice and environmental harm cases and suggest that courts that have refused to recognize increased-risk standing have improperly applied the law.[140]

These arguments raise important considerations in the discussion surrounding data breach standing. However, in proposing a framework by which to analyze a future injury, these arguments overlook the existing, actual injury of the theft of plaintiffs' personal information. In doing so, these arguments are promoting a theory of standing whereby courts are asked to predict the future rather than addressing an injury that has already occurred.[141] What's more, the increased-risk approach raises questions about whether the injury is fairly traceable to the defendant. To construe the injury as occurring when there has been fraudulent misuse is to intertwine the injury with the acts of third parties who are not present in the litigation.[142] In contrast, to construe the injury as occurring when the data has been stolen is to recognize that institutions are no more culpable for their negligent stewardship of consumer data when the data has been misused than they are when the data has been stolen. Moreover, advocating for recognition of increased-risk standing overlooks precedent in the First,[143] Third,[144] Fourth,[145] and Eighth Circuits[146] that would make it difficult for plaintiffs to establish standing based on increased risk. Given the Supreme Court's reluctance to address the issue thus far, it would be prudent for trial and appellate courts to adopt a framework that comports with existing law and ensures fairness and consistency for future data breach plaintiffs.

Thus, courts should shift the standing inquiry to the inherent injury of the data breach. When plaintiffs can show that their information was stolen in a data breach, courts should recognize the theft as an injury-in-fact sufficient to support standing because (1) Supreme Court jurisprudence supports recognition of such an injury, and (2) the injury comports with the principles that underlie the doctrine of standing.

---

[139] Galbraith, *supra* note 79, at 1398.

[140] *Id.* at 1387, 1398.

[141] *See* Beatty, *supra* note 21, at 1303 (arguing that courts should not be asked to predict the future).

[142] *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 392 (6th Cir. 2016) (Batchelder, J., dissenting) ("If [Plaintiffs] suffered injury, it was at the hands of criminal third-party actors, and their complaints do not make the factual allegations necessary to fairly trace that injury to [Defendant].").

[143] Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012).

[144] Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

[145] Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

[146] *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017).

B. Courts Should Recognize the Inherent Injury of the Data Breach as Sufficient to Support Standing

1. Supreme Court Jurisprudence

Supreme Court jurisprudence supports recognition of the inherent injury of the data breach. In order to properly allege an injury-in-fact, a plaintiff must show that she has suffered an "invasion of a legally protected interest,"[147] and that the harm is "actual or imminent" and "concrete and particularized."[148] Under the principles set forth in *Clapper* and *Spokeo*, the inherent injury of the data breach qualifies as an injury-in-fact because (a) the theft represents an actual—not imminent—harm, and (b) the injury is both concrete and particularized.

(a) Actual or Imminent

To properly allege an injury-in-fact, a plaintiff must show that she has suffered an "actual" injury that has already occurred or is ongoing, or that she will suffer an "imminent" injury.[149] If a plaintiff alleges a threatened injury that has not yet occurred, courts must employ the analysis set forth in *Clapper* to determine whether the threatened injury is "certainly impending," or whether it is merely "speculative."[150] However, if a plaintiff alleges an injury that is ongoing or has already occurred, courts must determine whether that "actual" injury is "concrete and particularized" under *Spokeo*.[151]

For data breach plaintiffs, courts have traditionally analyzed an injury based on the increased risk of identity theft. Accordingly, courts have utilized the analysis in *Clapper* to determine whether identity theft is "certainly impending" in the aftermath of a data breach.[152] But this inquiry is unnecessary when courts recognize an injury based on the theft of plaintiffs' personal information, irrespective of potential fraudulent misuse of that information. When courts analyze standing based on the "actual" injury of the stolen data, the inquiry should proceed to whether that injury is both "concrete" and "particularized" under *Spokeo*.[153]

---

[147] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

[148] Monsanto Co. v. Geerston Seed Farms, 561 U.S. 139, 149 (2010).

[149] Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 472 (1982) (citation omitted).

[150] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410, 414 (2013).

[151] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

[152] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2016) (relying on *Clapper* to hold that future identity theft was not certainly impending following the theft of a hospital laptop containing sensitive personal information).

[153] *Spokeo*, 136 S. Ct. at 1548.

(b) Concrete and Particularized

A properly alleged injury-in-fact must be both "concrete and particularized."[154] An injury is "particularized" when it affects the plaintiff "in a personal and individual way."[155] An injury is "concrete" when it is "real" or "actually exists" and is not "abstract."[156] An intangible harm may be a "concrete" injury when it "has a close relationship to a harm that has traditionally . . . provid[ed] a basis for a lawsuit in English or American courts,"[157] or when Congress has manifested an intent to "elevat[e]" the intangible harm "to the status of [a] legally cognizable injur[y]."[158]

For plaintiffs bringing suit in the aftermath of a data breach, there is little doubt that the theft of their personal information is a "particularized" injury that affects them "in a personal and individual way." In the wake of a data breach, victims incur both financial and emotional harms.[159] For example, the *Galaria* plaintiffs alleged that:

> [They] "have suffered, and will continue to suffer" costs—both "financial and temporal"—that include "purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts."[160]

Given the highly personal nature of the information stolen, in concert with the very real threat of fraudulent misuse of that data, there is little question that theft of personal information represents a "particularized" injury. The critical question, then, is whether the theft of personal information during an institutional data breach is a "concrete" injury.

A "concrete" injury is easily recognizable when a plaintiff has suffered physical or financial harm.[161] When plaintiffs have suffered these sorts of tangible harms, the issue of concreteness is generally not even disputed.[162] However, as the Supreme Court noted in *Spokeo*, an intangible harm may qualify as a concrete injury.[163] Indeed, courts have long been willing to recognize intangible injuries in actions such as trespass, defamation, and breach of contract.[164] In determining whether an

---

[154] *Id.*

[155] *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 n.1 (1992)).

[156] *Id.*

[157] *Id.* at 1549.

[158] *Id.* (quoting *Lujan*, 504 U.S. at 578).

[159] Galbraith, *supra* note 79, at 1369.

[160] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386–87 (6th Cir. 2016) (citations omitted).

[161] Beatty, *supra* note 21, at 1295.

[162] *Id.*

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

[164] Beatty, *supra* note 21, at 1295.

intangible injury may qualify as a concrete injury, it is instructive to look to history and consider whether the alleged injury bears a relation to a harm that has "traditionally . . . provid[ed] a basis for a lawsuit in English or American courts."[165] Additionally, for plaintiffs alleging statutory violations, courts may consider whether Congress intended to "elevat[e] the status" of the intangible harm encompassed in the statute to a "legally cognizable" injury sufficient to confer standing.[166]

For example, in *In re Horizon Healthcare Services Inc. Data Breach Litigation*,[167] the Third Circuit determined whether data breach plaintiffs had Article III standing by applying the concreteness analysis set forth in *Spokeo*. In *Horizon*, plaintiffs brought suit against their health insurer after two laptops containing plaintiffs' unencrypted personal information were allegedly stolen from the insurer's headquarters.[168] The plaintiffs asserted common-law claims such as negligence, breach of contract, and invasion of privacy, as well as violations of the FCRA.[169] Importantly, the *Horizon* plaintiffs argued that the unauthorized disclosure of their personal information was, in and of itself, an injury-in-fact.[170] The Third Circuit applied the two-part concreteness test set forth in *Spokeo*, looking both to "history and the judgment" of Congress.[171] The court ultimately granted standing based on the alleged violations of the FCRA.[172] However, the reasoning employed in both the majority and concurring opinions is valuable in assessing whether the theft of personal information may qualify as a concrete injury in the context of statutory violations *or* common-law claims.

Looking first to history, the Third Circuit noted that "'unauthorized *disclosures* of information' have long been seen as injurious."[173] Hearkening to common-law privacy torts, the court noted that improper dissemination of information can represent a concrete, cognizable injury.[174] Indeed, the court cited to the Restatement (Second) of Torts, which states that "[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other."[175] Although the majority noted that the unauthorized disclosure of personal information resulting from a data breach was closely related to privacy torts long recognized in English and American courts, they concluded that the defendant's

---

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

[166] *Id.* (citing *Lujan*, 504 U.S. at 278).

[167] 846 F.3d 625 (3d Cir. 2017).

[168] *Id.* at 630.

[169] *Id.* at 631 & n.4.

[170] *Id.* at 634. Plaintiffs also alleged an increased-risk theory of standing, however the court did not find it necessary to address that theory. *Id.* at 634–35.

[171] *Id.* at 637.

[172] *Id.* at 635.

[173] *Id.* at 638 (quoting *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 274 (3d Cir. 2016)).

[174] *Id.*

[175] *Id.* (citing Restatement (Second) of Torts § 652A (Am. Law Inst. 1977)).

actions would not "give rise to a cause of action under common law."[176] However, the court turned next to the judgment of Congress, finding that the passage of the FCRA showed that Congress intended to elevate the status of the unauthorized dissemination of personal information to a "concrete," "legally cognizable" injury-in-fact.[177] Thus, the Third Circuit granted Article III standing for data breach plaintiffs based on the inherent injury of the breach itself, irrespective of the likelihood of future identity theft.[178]

For many data breach plaintiffs, the Third Circuit's reasoning in *Horizon* will serve as a promising guidepost. Given the availability of the FCRA, many data breach plaintiffs will likely be able to establish Article III standing by pointing to the judgment of Congress. However, because the FCRA is targeted to "consumer reporting agencies,"[179] it will not be an appropriate cause of action in every data breach case. Although data breach plaintiffs have successfully alleged violations of the FCRA in the context of breaches at insurance companies,[180] it is easy to see how the victims of a data breach at a retail organization or service provider could be disadvantaged simply because of the nature of the organization that failed to protect their data. Some commentators have proposed statutory solutions that would "elevate the status" of a data breach to a concrete injury.[181] Although a legislative solution would certainly promote justice and access to the courts for data breach plaintiffs, these arguments are subject to the political realities associated with passing a comprehensive data breach statute.[182] Given the inefficiency and uncertainty associated with congressional action, it would be prudent for courts to adopt a sensible judicial solution that comports with existing Supreme Court jurisprudence and does not conflict with circuit precedent.[183] Accordingly, courts should recognize the theft of personal information in a data breach as a concrete injury sufficient to confer standing.

Given the close relationship between the theft of personal information and common-law privacy torts, courts may properly recognize the theft of personal information as a concrete injury. As the Third Circuit noted in *Horizon*, the common law has historically permitted claims based on invasions of privacy even when the

---

[176] *Id.* at 639 ("No common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive.").

[177] *Id.* at 639 & n.19.

[178] *Id.*

[179] 15 U.S.C. § 1681(a)(4) (2016) ("There is a need to insure [sic] that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."); *id.* § 1681(a)(f) (defining consumer reporting agency).

[180] *See Horizon*, 846 F.3d at 631; Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385 (6th Cir. 2016).

[181] Lorio, *supra* note 19.

[182] Martecchini, *supra* note 18, at 1494.

[183] The Third Circuit's recognition of the inherent injury of the data breach did not conflict with circuit precedent rejecting increased-risk standing. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42–43 (3d Cir. 2011).

plaintiff cannot prove actual damages.[184] For example, a plaintiff may bring a claim for defamation without proving any specific harm to her reputation.[185] Likewise, damages are available for privacy torts "in the same way in which general damages are given for defamation," without proof of "pecuniary loss [or] physical harm."[186] In the context of data breach litigation, the theft of personal information during a breach bears a close relationship to long-recognized privacy torts. Just as actual harm in privacy torts is a question of damages rather than a question of injury-in-fact, the risk of future identity theft in data breach cases should be a matter of damages, rather than a potential bar to Article III standing.

Moreover, courts should recognize the inherent injury of the data breach as a concrete injury because the theft of personal information is a violation of a private right, rather than a public right. Private rights are those rights "belonging to individuals, considered as individuals," historically including rights of personal security and reputation, property rights, and contract rights.[187] When a plaintiff brings suit for the violation of a private right, courts have historically found that the plaintiff suffered a concrete, *de facto* injury "merely from having [her] personal, legal rights invaded."[188] Accordingly, plaintiffs asserting the violation of private rights have not historically been required to show additional harm to establish a "case or controversy."[189] In contrast, courts have typically required a showing of additional harm when plaintiffs allege violations of public rights.[190] Public rights are those that involve duties owed "to the whole community, considered as a community, in its social aggregate capacity."[191] For example, in a public nuisance suit, a plaintiff must allege "special, individualized damage" as a result of the nuisance in order to seek relief for "an otherwise public-rights claim."[192] Because the theft of personal information represents a private right and is closely related to common-law tort claims, courts should recognize the theft of personal information as a concrete injury.

In the wake of an institutional data breach, plaintiffs may bring suit based on the theft of their personal information. When plaintiffs can show that their information has been stolen, courts should apply the Article III standing analysis set forth in *Clapper* and *Spokeo* to determine whether the theft represents an injury-in-fact sufficient to confer standing. Because the theft of plaintiffs' personal

---

[184] *Horizon*, 846 F.3d at 642 (Shwartz, J., concurring).

[185] Doe v. Chao, 540 U.S. 614, 621 n.3 (2004) (citing RESTATEMENT OF TORTS § 621 cmt. a (AM. LAW INST. 1938) ("It is not necessary for the plaintiff [who is seeking general damages in an action for defamation] to prove any specific harm to his reputation or any other loss caused thereby")).

[186] *Id.* (quoting Restatement (Second) of Torts § 867 cmt. d (Am. Law Inst. 1939)).

[187] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1551 (2016) (Thomas, J., concurring) (quoting 3 WILLIAM BLACKSTONE, COMMENTARIES *2).

[188] *Id.*

[189] *Id.*

[190] *Id.*

[191] *Id.* (quoting 4 WILLIAM BLACKSTONE, COMMENTARIES *5).

[192] *Id.* (citing 3 WILLIAM BLACKSTONE, COMMENTARIES *220).

information is an "actual" injury that is both "particularized" and "concrete," courts should grant standing based on the inherent injury of the data breach.

2. Principles of Standing

The final step in determining whether courts should recognize the inherent injury of the data breach is to consider whether doing so would violate the principles that underlie the doctrine of standing. The Supreme Court has developed the doctrine of standing to support Article III's "case or controversy" requirement. More specifically, requiring a plaintiff to show that she has standing to sue is meant to ensure the "properly limited . . . role of the courts in a democratic society"[193] and to "prevent the judicial process from being used to usurp the powers of the political branches."[194] When a dispute would require the court to "decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional," the court's standing inquiry will be "especially rigorous."[195] However, "when a private plaintiff seeks to enforce only [her] personal rights against another private party," concern about the judiciary's entanglement in political disputes is generally absent.[196]

Data breach litigation typically takes the form of private individuals suing to redress their own private rights. In this context, there is no threat of judicial entanglement in political disputes, nor is there concern about the judiciary usurping political powers. Indeed, in the context of data breach litigation, there is no danger that the suit "is an impermissible attempt to police the activity of the political branches."[197] By recognizing the inherent injury of the data breach, courts do not run the risk of violating the separation-of-powers principles that underlie the doctrine of standing.

CONCLUSION

As services like healthcare, banking, and retail shopping become increasingly digitized, consumers will continue to entrust institutions with their sensitive, personal information. With data breaches on the rise, consumers' personal information will remain under constant threat of compromise. In the aftermath of these breaches, victims will continue to turn to the courts to seek redress for the violation of their privacy and the disruption of their trust. In order to be heard in federal court, data breach plaintiffs will need to show that they have suffered an injury-in-fact sufficient to support Article III standing.

Courts have divided on whether to grant standing based on the increased risk of identity theft in the wake of a data breach. In order to ensure predictability and

---

[193] Warth v. Seldin, 422 U.S. 490, 498 (1975).
[194] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).
[195] Raines v. Byrd, 521 U.S. 811, 819–20 (1997).
[196] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1551–53 (2016) (Thomas, J., concurring).
[197] *Id.* at 1553.

justice for future data breach plaintiffs, courts should shift the injury-in-fact inquiry to the theft of plaintiffs' personal information, irrespective of future misuse of that information. Based on the requirements set forth in *Clapper* and *Spokeo*, and in accordance with the principles that underlie the doctrine of standing, courts should recognize the inherent injury of the data breach as an injury-in-fact sufficient to confer Article III standing.