William & Mary Bill of Rights Journal

Volume 29 (2020-2021)
Issue 3 The Presidency and Individual Rights

Article 9

March 2021

Article III Standing, the Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs

R. Andrew Grindstaff

ARTICLE III STANDING, THE SWORD AND THE SHIELD: RESOLVING A CIRCUIT SPLIT IN FAVOR OF DATA BREACH PLAINTIFFS

R. Andrew Grindstaff*

INTRODUCTION

"In fashion, one day you are in, and the next day you are out."[1] Much like the fashion industry, the contours of modern standing doctrine shift rapidly and, often times, confusingly. Standing doctrine has been described as "a jumbled mess,"[2] "mystifying,"[3] and an "escape hatch."[4] Though convoluted it may be, the complexity of standing doctrine illustrates above all its nature as nothing more than a construct of the judiciary.

The law is complicated, and judges' attempts to craft bright-line rules to interpret and apply the law tend to muddle, rather than clarify, the purpose of the law in question.[5] So, too, with standing doctrine. The modern standing doctrine test has been reduced to three "minimum" requirements,[6] implying a hard-and-fast rule to shield the judiciary from cases it might not wish to hear; however, tracing the

---

* JD Candidate, William & Mary Law School, 2021; BA, University of Virginia, 2014. Thank you to my mother, Suzanne, for her unwavering support, and to my father, Charles, in whose memory this Note is dedicated.

[1] This catchphrase, attributed to the host of *Bravo*'s fashion design reality television show, *Project Runway*, references the quick, unpredictable shifts in the trend *du jour* of the fashion industry. *See* Kate Aurthur, *Another Catwalk for Fashion Series*, N.Y. TIMES (Dec. 6, 2005), https://www.nytimes.com/2005/12/06/arts/another-catwalk-for-fashion-series.html [https://perma.cc/S7KH-CABW].

[2] John A. Ferejohn & Larry D. Kramer, *Independent Judges, Dependent Judiciary: Institutionalizing Judicial Restraint*, 77 N.Y.U. L. REV. 962, 1010 (2002).

[3] Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 170 (2012).

[4] Eugene Kontorovich, *Legal 'Standing': Obama's Executive Branch Escape Hatch*, L.A. TIMES (Mar. 2, 2014, 12:00 AM), https://www.latimes.com/opinion/op-ed/la-oe-kontorovich-obamacare-legal-standing-20140302-story.html [https://perma.cc/3MZN-5FDY].

[5] *See* Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953, 991–96 (1995) (noting several flaws with attempts to craft rules of law); *see also* John F. Duffy, *Rules and Standards on the Forefront of Patentability*, 51 WM. & MARY L. REV. 609, 614 (2009) ("[F]or patentable subject matter . . . rules always fail."). *See generally* Steven J. Mulroy, *The Bright Line's Dark Side: Pre-Charge Attachment of the Sixth Amendment Right to Counsel*, 92 WASH. L. REV. 213 (2017) (arguing against bright-line rules when considering pre-charge Sixth Amendment right to counsel issues).

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

development of the modern doctrine reveals these minima as rather a sword for litigants to address ahistorical wrongs.[7] Framing standing doctrine as solely protection for the courts unnecessarily—and perhaps unconstitutionally—excludes individuals who have suffered abstract, but not generalized, wrongs from access to judicial redress.[8] Fortunately, when courts fabricate tests from whole cloth, those tests are easily redesigned when the trend *du jour* turns to *faux pas*.

The recent proliferation of data breaches[9] is one such event requiring a rethreading of standing doctrine. The Courts of Appeal are currently split on whether to allow or deny standing for data breach plaintiffs[10]—those persons seeking recourse from the entities that fell victim to the breach and therein lost plaintiffs' data to an unknown third party. Standing requires plaintiffs to show some injury,[11] and how courts approach the concept of injury in these data breach cases determines whether plaintiffs will survive the standing analysis.[12] Despite the disparate treatment of litigants across the circuits, the Supreme Court has repeatedly punted when asked to resolve the issue.[13] Because of the grave importance of data breach plaintiffs' lost and stolen data,[14] the Court must relinquish its standing shield and hand these litigants a sword to pursue remedy.

Part I of this Note discusses the origin of the standing doctrine and its modern articulation. Part II maps out the current condition of data breach litigation standing

---

[7] *See infra* Section I.A.

[8] *See infra* Section I.B.

[9] *See, e.g.*, Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#3da86375bd54 [https://perma.cc/SS3C-8T6W]; Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds*, NBC NEWS (July 24, 2017, 10:18 AM), https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881 [https://perma.cc/Z8NQ-XHH2].

[10] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).

[11] *Lujan*, 504 U.S. at 560–61 (establishing the three-part test: injury, nexus, and redressability).

[12] *See* Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 695 (2017) ("Out of the three prongs of Article III . . . plaintiffs most often falter on establishing injury . . . ."). *But see* Aaron Wynhausen, Note, *The Eighth Circuit Further Complicates Plaintiff Standing in Data Breach Cases*, 84 MO. L. REV. 297, 305–06 (2019) (noting that plaintiffs passing the injury threshold then might stumble on the redressability prong).

[13] *See, e.g.*, Frank v. Gaos, 139 S. Ct. 1041 (2019) (remanding for briefing on standing in light of the decision in Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)); *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[14] *See* Weisbaum, *supra* note 9 (noting that modern hackers target Social Security numbers and health records because they are worth significantly more on resale than credit card numbers).

in the Supreme Court and the Courts of Appeal. Part III attempts to resolve the circuit split by working through areas of agreement and open questions, arguing that a "breach alone" may be tolerable to every circuit. Part IV recommends potential solutions to the data breach standing issue, advancing a "tiered sensitivity" approach as the most preferable. Part V outlines foundational frameworks on which to base the solutions from both domestic and foreign jurisdictions and pleads for Court intervention despite congressional inaction.

I. ARTICLE III & STANDING

A. The Court's "Limits"

Constraints on the federal judiciary's power to adjudicate cases are largely, if not entirely, self-imposed limitations.[15] As part of establishing a judicial branch coequal to the executive and legislature, Article III of the Constitution provides two restrictions on the Court's authority to hear judicial matters.[16] First, federal courts may only hear actual "cases" or "controversies" implicating U.S. laws or citizens.[17] Second, aside from the Court's original jurisdiction, Congress may strip the Court of jurisdiction.[18]

Debate abounds as to the correct interpretation of both restrictions.[19] But ultimately, regardless of the many theories about the Court's power, "It is emphatically the province and duty of the judicia[ry] . . . to say what the law is."[20] Indeed, as early as *Marbury v. Madison*, the Court recognized its own obligation to curb the seemingly quite broad grant of discretionary constitutional power so as to balance the federal tripartite.[21] The Court has since developed a number of doctrines to limit its own adjudicative scope.[22]

---

[15] *See* Ferejohn & Kramer, *supra* note 2, at 1004 ("The federal judiciary . . . invent[ed] a whole series of doctrinal constraints that significantly reduce the scope of its potential authority.").

[16] *See* U.S. CONST. art. III, § 2.

[17] *See id.*; *Spokeo*, 136 S. Ct. at 1547.

[18] *See* U.S. CONST. art. III, § 2; *The Supreme Court, 1995 Term—Leading Cases*, 110 HARV. L. REV. 135, 277 (1996).

[19] *See* John Harrison, *The Power of Congress to Limit the Jurisdiction of Federal Courts and the Text of Article III*, 64 U. CHI. L. REV. 203, 205–08 (1997) (summarizing several arguments about the Cases or Controversies Clause); *The Supreme Court, 1995 Term—Leading Cases*, *supra* note 18, at 277 ("For years, commentators have debated whether Congress's power . . . is as far-reaching as the text of the Exceptions Clause seems to suggest . . . .").

[20] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803).

[21] *See id.* at 175–80 (refusing to issue writ of mandamus on jurisdictional grounds); Lee & Ellis, *supra* note 3, at 185–86, 186 n.94 (noting Hayburn's Case, 2 U.S. (2 Dall.) 409 (1792), as an earlier example of self-limitation not tied to the Constitution).

[22] *See* Allen v. Wright, 468 U.S. 737, 750 (1984) (abrogated on other grounds) (identifying "standing . . . mootness, ripeness, [and] political question" as Article III doctrines that "relate

Among these, standing doctrine addresses the Court's aversion to hearing generalized grievances.[23] Modern standing doctrine emerged in response to the expansion of the administrative state in the early to mid-20th century.[24] The precursor to modern standing doctrine required litigants to identify an existing common law interest to bring suit, rather than simply allege some harm.[25] In effect, persons harmed by a regulation were left without standing to challenge it unless that regulation interfered with a recognized interest in the common law.[26] In 1970, the Court abandoned fitting a square peg into a round hole and allowed standing where litigants suffered an Article III "injury in fact" and fell within a regulation's "zone of interests."[27]

To further entangle and manipulate the conception of standing, the Court also developed prudential considerations which may, separately from the question of constitutional standing, bar plaintiffs from bringing suit.[28] The first articulation of prudential standing came shortly after the Court's shift toward the injury in fact standing requirement.[29] In *Warth v. Selden*, the Court established the first two categories of prudential standing: first, denying plaintiffs access to the courts for "generalized grievance[s]," and second, disallowing plaintiffs to assert the rights of third parties.[30]

Approximately twenty years later, the Court pronounced the modern articulation of constitutional standing in *Lujan v. Defenders of Wildlife*, requiring an injury in fact, causation, and the potential for redress by the adjudicating court.[31] Conspicuously, "zone of interests" is not mentioned in the Court's *Lujan* opinion.[32] But only five years after *Lujan*, the Court confirmed the third category of prudential standing: zone of interests.[33]

---

in . . . overlapping ways . . . about the constitutional and prudential limits" of the Court (quoting Vander Jagt v. O'Neill, 699 F.2d 1166, 1178–79 (D.C. Cir. 1983) (Bork, J., concurring))).

[23] *See* Lee & Ellis, *supra* note 3, at 183.

[24] *See* Ferejohn & Kramer, *supra* note 2, at 1009–10; Cass R. Sunstein, *Standing and the Privatization of Public Law*, 88 COLUM. L. REV. 1432, 1446 (1988) ("[The Court's shift] responded to a belief that the private-law model no longer worked in public-law cases.").

[25] *See* Sunstein, *supra* note 24, at 1434–36.

[26] *See id.* at 1434–35; *see also* Ferejohn & Kramer, *supra* note 2, at 1010 ("[T]his private law model proved too unforgiving . . . .").

[27] *See* Ass'n of Data Processing Serv. Orgs. v. Camp, 397 U.S. 150, 152–53 (1970) ("The question of standing is different. It concerns, apart from the 'case' or 'controversy' test, the question whether the interest sought to be protected . . . is arguably within the zone of interests to be protected or regulated by the statute or constitutional guarantee in question.").

[28] *See* Ferejohn & Kramer, *supra* note 2, at 1010–11.

[29] *See* Warth v. Seldin, 422 U.S. 490, 498–501 (1975) (discussing the distinction between Article III requirements and "prudential considerations"); Kylie Chiseul Kim, *The Case Against Prudential Standing: Examining the Courts' Use of Prudential Standing Before and After* Lexmark, 85 TENN. L. REV. 303, 319–22 (2017).

[30] *See* Kim, *supra* note 29, at 321–22 (quoting *Warth*, 422 U.S. at 499).

[31] *See* 504 U.S. 555, 560–61 (1992).

[32] *See generally id.*

[33] Bennett v. Spear, 520 U.S. 154, 162 (1997) ("Numbered among these prudential requirements is the doctrine of . . . zone of interests . . . .").

The Court's shift in utilization of the zone of interests doctrine is indicative of the malleability of standing doctrine as a whole. Even better exemplified by the Court's recent elimination of the zone of interests doctrine altogether is *Lexmark International, Inc. v. Static Control Components, Inc.*[34] There, the Court explicitly relegated the zone of interests inquiry to utilization in determining whether the plaintiff has a cause of action, not standing.[35] While leaving intact the original two prudential considerations,[36] *Lexmark* arguably signaled the Court's willingness to revisit issues of, at least, prudential standing, which may underscore a willingness to rethink constitutional standing in certain contexts.

But the Court's original shift in approach to standing—moving from identifiable cause of action to identifiable injury—necessarily flipped the doctrine from a shield for the judiciary into a sword for plaintiffs to redress nontraditional harms. In doing so, the Court tipped its hand and reminded observers that standing is not only malleable, but nothing more than an artifice of the Court's own design. The Court has continuously emphasized that fact in its maddeningly inconsistent treatment of standing over the last half century.[37] Faced with the square peg of defining harm in a data breach, the Court should capitalize on the circuit split opportunity to adapt standing doctrine into a sword for digital age litigants.

B. Articulating Modern Constitutional Standing Doctrine

Illustrative of the uncertainty inherent in the modern formulations of standing doctrine, when pronouncing the zone of interests requirement in *Ass'n of Data Processing Service Organizations, Inc. v. Camp*,[38] the Court failed to articulate the contours of its application.[39] The lower circuits struggled to reach consensus on the issue, forcing the Court to later explain that the test merely guided courts when a litigant challenged a regulation to which it is not directly subject.[40] And during this

---

[34] *See* 572 U.S. 118, 127 (2014) ("Although we admittedly have placed [the zone of interests] test under the 'prudential' rubric in the past, it does not belong there . . . .") (citation omitted); Kim, *supra* note 29, at 335–36.

[35] *See Lexmark*, 572 U.S. at 127–28; Kim, *supra* note 29, at 336.

[36] *See* Kim, *supra* note 29, at 336–37 (noting *Lexmark* spoke only to zone of interests and third-party rights considerations, leaving open the question of whether the latter should also be stripped of its prudential label).

[37] *See generally supra* notes 23–36 and accompanying text.

[38] *See* 397 U.S. 150, 153–56 (1970).

[39] *See, e.g.*, Bennett v. Spear, 520 U.S. 154, 162–63 (1997) (noting that the requirement applied broadly after *Data Processing* and only later was affirmatively bounded); *see also* Jonathan R. Siegel, *Zone of Interests*, 92 GEO. L.J. 317, 321 (2004).

[40] *See* Clarke v. Sec. Indus. Ass'n, 479 U.S. 388, 399–400 (1987); Siegel, *supra* note 39, at 322–25. In effect, suggests Siegel, the Court considered the zone of interests requirement a general prudential concern, not tied to a specific statute at issue. *See id.* at 328.

time, the Court also added to the Article III injury in fact requirement,[41] culminating in the modern articulation provided in *Lujan v. Defenders of Wildlife*.[42]

In *Lujan*, an environmental advocacy group brought suit against the Department of the Interior (DOI).[43] The plaintiffs sought reversal of a DOI rule that interpreted a section of the Endangered Species Act as only applying, effectively, "within the United States."[44] The plaintiffs claimed an injury through loss of habitat for endangered species abroad, which would cause extinction of those species, and, therefore, interested parties could no longer study or visit those species.[45] The Court denied the plaintiffs standing due to insufficient demonstration of an imminent injury.[46]

The modern doctrine infers from the language of Article III "irreducible constitutional minimum" requirements to maintain a suit in federal court.[47] To achieve constitutional standing, a plaintiff must allege (1) an injury in fact; (2) a nexus between the injury and some conduct by the defendant; and (3) redressability of the injury through a favorable decision.[48]

1. Injury in Fact

The Court developed the injury in fact prong alongside the zone of interests requirement in *Data Processing* simply as a means of shifting standing analysis away from the traditional "legal interest" concept and toward recognition of *any* factual harm—to expand, rather than curtail, the scope of recognized injuries for standing purposes.[49] Since *Data Processing*, however, the Court has chipped away at that expansion to (presumably) ensure both that the judiciary remains constrained with respect to its coequal branches and that the judicial system reserves its scant administrative bandwidth to adjudicate only the clearest cases of injury.[50]

---

[41] Siegel, *supra* note 39, at 320.

[42] *See* 504 U.S. 555, 560–61 (1992).

[43] *Id.* at 559.

[44] *Id.* at 557–59.

[45] *Id.* at 563–64.

[46] *Id.* at 564.

[47] *Id.* at 560.

[48] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan*, 504 U.S. at 560–61).

[49] *See* Ass'n of Data Processing Serv. Orgs. v. Camp, 397 U.S. 150, 152–54 (1970); F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 289–90, 295 (2008) (second alteration in original) ("[T]he Court intended to 'expand [ ] the types of "personal stake(s)" which are capable of conferring standing . . . .'" (quoting Linda R.S. v. Richard D., 410 U.S. 614, 616–17 (1973))).

[50] *See* Rachel Bayefsky, *Constitutional Injury and Tangibility*, 59 WM. & MARY L. REV. 2285, 2296–97 (2018); *see also* Hessick, *supra* note 49, at 300 ("So, why does current standing doctrine require injury in fact? The most likely reason is that it is firmly entrenched in the law.").

But the Court continually justifies the rationale of injury in fact as a requirement of Article III,[51] despite Article III's text demanding no such prerequisite to adjudication.[52] The murkiness of the injury in fact prong precisely encapsulates why the standing doctrine as a whole continually causes problems with persistently modern issues like data breaches. Today, plaintiffs prove injury in fact by showing "'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent . . . .'"[53] But, put simply, the boundaries and meaning of the injury in fact requirement remain vastly unsettled and open to revision despite repeated Court attempts to clarify.

a. Actual or Imminent

The first injury in fact question asks whether a harm is "actual or imminent, not 'conjectural' or 'hypothetical.'"[54] An actual injury, for the purpose of contrasting with an imminent threat, need not be physical or visible, but simply the "invasion of a legally protected interest."[55] Recently the Court reiterated its adherence to this principle, quoting dicta from *Lujan* that describes the necessary injury as "not too speculative."[56] In other words, a "threatened injury must be *certainly impending*" to constitute Article III standing and "[a]llegations of *possible* future injury" are insufficient.[57]

According to the Court, an imminent injury may rest on a chain of inferences so long as that chain is sufficiently connective and not too attenuated.[58] However, the Court did not speak to what exactly constitutes too much attenuation.[59] More recently, the Court clarified that the concreteness requirement of injury in fact may be satisfied by "risk of real harm," which in turn suggests that the imminence requirement should be subject to the same treatment—turning on the probability of injury rather than the actuality (in time and space) of injury.[60] But this point remains unsettled.

---

[51] *See* Hessick, *supra* note 49, at 300.

[52] *See* U.S. CONST. art. III, § 2.

[53] *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560).

[54] *Lujan*, 504 U.S. at 560 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

[55] *See id.*; *see also* F. Andrew Hessick, *Understanding Standing*, 68 VAND. L. REV. EN BANC 195, 196 (2015).

[56] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting *Lujan*, 504 U.S. at 565 n.2).

[57] *Id.* (quoting *Whitmore*, 495 U.S. at 158).

[58] *See id.* at 414 & n.5 (noting the Court's grant of standing for a "substantial risk" of future injury and the potential of distinction between substantial risk and "certainly impending" injury (citations omitted)).

[59] *See id.* at 411–14 (rejecting plaintiffs' attempted trace between threatened injury and defendant's conduct, but not pronouncing a test).

[60] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness."); *see also* Lee & Ellis, *supra* note 3, at 179–80 (noting the Court's vacillation on the subject and assuming *arguendo* that the Court intends for imminence to involve both "temporality and probability").

b. Concrete and Particularized

In a recent decision, the Court distinguished that the second injury in fact question operated as a conjunctive—that concreteness and particularization are separate concepts, each of which much be satisfied to successfully survive analysis.[61] To be particular, an injury "must affect the plaintiff in a personal and individual way."[62] To be concrete, an "injury must be '*de facto*'"[63]—"'real,' and not 'abstract.'"[64]

But a concrete injury need not be tangible.[65] When an alleged harm is intangible, the Court suggested that both historical common law claims and Congress's wisdom can inform, but not obligate, which of those harms will suffice for the standing analysis.[66] Thus, threat of future injury could be a concrete harm either by reference to traditional claims or a federal statute.[67] The Court further explained that violation of a congressional procedural right alone may survive the injury in fact inquiry.[68] But ultimately, the "last word" on concreteness rests with the judiciary, and, for now, lower courts wrestle with that duty given the Court's disheveled explanation of tangibility.[69]

2. Nexus

The second prong of modern standing doctrine developed as a logically necessary counterpart to the injury in fact requirement.[70] If a litigant suffers a factual Article III harm, that harm must come at the hands of some other person or entity, otherwise a plaintiff must sue him- or herself. Thus, the Court pronounced that a plaintiff must allege "a causal connection between the injury and [defendant's] conduct" where the harm is "fairly . . . trace[able] to the challenged action of the defendant, and

---

[61] *Spokeo*, 136 S. Ct. at 1548 ("Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be concrete.") (internal quotation omitted).

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

[63] *Id.* (citing BLACK'S LAW DICTIONARY 479 (9th ed. 2009)).

[64] *Id.* (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 472 (1971); RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 305 (1967)).

[65] *Id.* at 1549.

[66] *See id.* (noting, as to the latter source, "Congress' [sic] role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a [private right of action]"). *But see* Michael C. Dorf, *Supreme Court Requires "Concrete" Injury for Standing*, VERDICT (May 18, 2016), https://verdict.justia.com/2016/05/18/supreme-court-requires-concrete-injury-standing [https://perma.cc/H5BU-4SJG] (arguing that the Court confused threshold standing with substantive liability by looking to Congress's historical recognition of injury).

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

[68] *See id.*; Bayefsky, *supra* note 50, at 2304.

[69] *See* Bayefsky, *supra* note 50, at 2304–05, 2308–09.

[70] *See* Lee & Ellis, *supra* note 3, at 180.

not . . . th[e] result [of] the independent action of some third party . . . ."[71] Similar to the imminence analysis, the chain of causation may not be too attenuated or speculative.[72] Because standing in data breach litigation turns almost entirely on proving injury in fact, this prong is discussed only in brief to provide context.

3. Redressability

Finally, a plaintiff must allege an injury for which it would be "'likely,' as opposed to merely 'speculative,'" that a ruling for the plaintiff will redress the harm.[73] Like the causation prong, the redressability prong is analyzed by reference to a chain of speculation and inference.[74] But the redressability prong is analytically distinct from the causation prong: the latter focuses on what defendant did to cause the harm; the former focuses on whether the requested relief will remedy the complained-of harm.[75] Redressability, like the nexus prong, is of little substantive value to analyze data breach litigation standing, so this discussion merely provides context for a holistic understanding of the Court's modern standing doctrine formulation.

II. CURRENT STATE OF STANDING IN DATA BREACH LITIGATION

Data breaches are by nature difficult to actualize into a justiciable injury.[76] Even defining "data" poses a challenge given its likely infinite number of forms and characterizations: vital (medical records), critical (Social Security numbers), financial (credit card numbers), etc.[77] In a typical data breach situation, a third party gains

---

[71] *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (alteration in original) (quoting Simon v. E. Ky. Welfare Rts. Org., 426 U.S. 26, 41–42 (1976)).

[72] *See* Lee & Ellis, *supra* note 3, at 180–82; *see also id.* at 580 (Kennedy, J., concurring in part) (leaving open the possibility that the extent of the chain may be defined by Congress (in addition to the courts)).

[73] *Lujan*, 504 U.S. at 561 (quoting *Simon*, 426 U.S. at 38, 43).

[74] *See* Lee & Ellis, *supra* note 3, at 182–83 (briefly discussing three Supreme Court decisions denying standing because redressability of the harm was too speculative).

[75] *See* Sprint Commc'ns Co. v. APCC Servs., Inc., 554 U.S. 269, 287 (2008) ("[T]o demonstrate redressability, the plaintiff must show a 'substantial likelihood that the requested relief will remedy the alleged injury in fact . . . .'" (emphasis removed) (quoting Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 771 (2000))).

[76] *See* Max Melio, Note, *Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation*, 61 B.C. L. REV. 1223, 1229–31 (2020) ("Fraudulent charges are the most concrete identity theft harm, but a number of more abstract harms have been noted as well. . . . There also may be new harms that materialize in the future.").

[77] One dictionary unhelpfully defines it as "information in digital form that can be transmitted or processed." *Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data [https://perma.cc/9KUE-AZJN] (last visited Mar. 15, 2021). The federal government broadly defines Personally Identifiable Information (PII)—which is often, but not always, digital—as any "information that can be used to distinguish or trace an individual's identity,

unauthorized access to a plaintiff's data by infiltrating a system—controlled by a defendant or another party—which a defendant uses to store that data.[78]

For the purposes of litigation, this situation poses a number of challenges, and chief among them is how to define the plaintiff's harm. Two recent Supreme Court cases—*Clapper v. Amnesty International USA*[79] and *Spokeo, Inc. v. Robins*[80]—form the basis for articulating a data breach injury despite neither case concerning a data breach in the "typical" sense (i.e., hackers penetrating digital infrastructure to obtain the plaintiffs' data). Unsurprisingly, the lower circuits developed a split when adapting the Court's "modern" standing articulation to these ultra-modern data breach situations. Some circuits contend that a threat of future identity theft suffices to form a cognizable injury in fact,[81] while others require some physical, tangible injury.[82]

A. Clapper *&* Spokeo

In *Clapper*, a group of plaintiffs comprising "attorneys and human rights, labor, legal, and media organizations" alleged that a statute allowing potential surveillance of their communications to clients outside of the United States, who "are likely targets of surveillance under [the statute]," caused harm to the plaintiffs.[83] The plaintiffs claimed injury from the statute because, among other things, the plaintiffs forewent telephone and email communications in favor of traveling to their clients' locations directly to circumvent the possibility of the U.S. government's surveillance.[84]

The Court denied the plaintiffs standing to recover those costs because the harm alleged by the plaintiffs was "not certainly impending."[85] Therefore, the Court's disposition focused on the imminence of the future risk of harm.[86] Because the plaintiffs' fear of surveillance was not proven to be imminent, the actual costs the plaintiffs

---

either alone or when combined." OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, PREPARING FOR AND RESPONDING TO A BREACH OF PERSONALLY IDENTIFIABLE INFO. 8 (2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf [https://perma.cc/BDL9-QDPA].

[78] Luke Irwin, *How Do Data Breaches Happen? Understanding Your Organisation's Biggest Threats*, IT GOVERNANCE (June 26, 2019), https://www.itgovernance.co.uk/blog/understanding-the-different-types-of-data-breaches [https://perma.cc/FMQ9-433Y] (categorizing and describing seven types of data breaches).

[79] 568 U.S. 398 (2013).

[80] 136 S. Ct. 1540 (2016).

[81] *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965–66 (7th Cir. 2016).

[82] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 768–70 (8th Cir. 2017).

[83] *See Clapper*, 568 U.S. at 406–07.

[84] *See id.* at 407 ("In addition, [plaintiffs] declare that they have undertaken 'costly and burdensome measures' to protect the confidentiality of sensitive communications." (citation omitted)).

[85] *See id.* at 416.

[86] *Id.* ("[R]espondents cannot manufacture standing by inflicting harm on themselves based on their fears of hypothetical future harm that is not *certainly impending*." (emphasis added)).

incurred to mitigate those fears were also non-imminent.[87] But the Court only held that the fear of a future harm must be nonspeculative; it did not foreclose that risk as insufficient to survive the imminence analysis.[88]

The defendant in *Spokeo* ran a digital "people search engine."[89] Given "a person's name, a phone number, or an e-mail address," the defendant's website crawled online databases to generate an information package about that person.[90] The plaintiff alleged that when the defendant's website compiled information about the plaintiff, all of the information the website returned was wrong, which constituted a "willful[] fail[ure] to comply with [a federal statute's] requirements."[91]

The Court remanded the case to the Ninth Circuit for further inquiry into whether the plaintiff adequately alleged both a particularized *and* concrete injury, given that, according to the Court, the Ninth Circuit inappropriately conflated the two concepts and failed to properly analyze the concreteness prong of injury in fact.[92] The Court took measured care to note that "a bare procedural violation," without more, cannot survive the concreteness analysis.[93] But the Court also deliberately emphasized that a risk of future harm remains viable in the standing analysis despite its intangibility.[94]

B. The Circuit Split

1. Expansive Theories

The Sixth, Seventh, Ninth, and D.C. Circuits have adopted plaintiff-friendly standing theories regarding injury in data breach litigation.[95] Generally, these courts

---

[87] *See id.* at 422.

[88] *See id.* at 416–18.

[89] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).

[90] *See id.*

[91] *Id.* at 1546.

[92] *See id.* at 1548, 1550.

[93] *See id.* at 1550 (noting that the defendant's website reporting "an incorrect zip code" posed little risk of actual harm). *But see* Dorf, *supra* note 66 (challenging the Court's minimization of the incorrect zip code by posing a hypothetical: if a potential employer mailed an employment solicitation to the zip code as reported, would plaintiff not have lost out on an employment opportunity?).

[94] *See Spokeo*, 136 S. Ct. at 1549 ("This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness." (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013))).

[95] *See generally In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016). It should be noted here that the Third Circuit has also granted standing to data breach litigants who brought suit under a federal statute. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 641 (3d Cir. 2017) ("Our precedent and congressional action lead us to conclude that the improper disclosure of one's personal data in violation of [a federal statute] is a cognizable injury for Article III standing purposes."). However, the court's analysis is grounded in congressional

agree that a heightened risk of identity theft following a data breach is sufficient for the purposes of Article III.[96] In each case, a third party hacked into a defendant's electronic system and stole the plaintiffs' personal data.[97]

The Seventh Circuit's analysis in *Lewert v. P.F. Chang's China Bistro, Inc.* is illustrative of the rationale employed in sister circuits.[98] In 2014, the defendant restaurant issued a public announcement that hackers had gained access to customer financial information.[99] When the plaintiffs learned of the breach and their potential exposure, they spent time, effort, and money to monitor their credit statements for identity theft and debit card accounts for fraudulent charges, and subsequently filed suit to recoup these losses.[100]

In granting standing to these plaintiffs, the court recognized that once a data breach has occurred and data is stolen, the risk of future harm from that loss is "concrete enough to support a lawsuit."[101] The court acknowledged that even without hackers utilizing the stolen data, the plaintiffs' time and effort spent mitigating potential losses are sufficient to support Article III standing.[102] Further expanding the reach of the plaintiffs' sword, the court noted that the reasonability of mitigation efforts is a question of merit, not standing.[103]

While *Lewert* illustrates the general approach of the expansive circuits, it is worth highlighting the D.C. Circuit's two-part "increased-risk-of-harm" test to emphasize the meaning of a *substantial* risk of future harm.[104] In 2014, the defendant health insurer fell victim to hackers who stole insureds' personal information, allegedly including names, birthdays, credit card numbers, Social Security numbers, and other health and sensitive information.[105] Reviewing the lower court's dismissal for lack of sufficiently alleged injury, the court applied a two-prong inquiry: (1) whether the "ultimate alleged harm" would be "concrete and particularized" and then (2) "whether the increased risk of such harm makes injury . . . sufficiently 'imminent.'"[106]

---

ability to grant standing through statute; therefore, this reasoning is analyzed *infra* in Section V.B. *See id.* at 635, 639–40.

[96] *See, e.g.*, *In re Zappos.com*, 888 F.3d at 1029; *see also Attias*, 865 F.3d at 627–29; *Galaria*, 663 F. App'x at 388–89; *Lewert*, 819 F.3d at 966–67.

[97] *In re Zappos.com*, 888 F.3d at 1023; *Attias*, 865 F.3d at 622; *Galaria*, 663 F. App'x at 386; *Lewert*, 819 F.3d at 965.

[98] *See generally Lewert*, 819 F.3d 963.

[99] *Id.* at 965.

[100] *See id.*

[101] *Id.* at 967.

[102] *Id.*

[103] *Id.*

[104] *See* Attias v. CareFirst, Inc., 865 F.3d 620, 627–29 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[105] *Id.* at 622–23, 628.

[106] *Id.* at 627 (quoting Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 915 (D.C. Cir. 2015)).

Because the plaintiffs alleged identity theft as the ultimate injury, which "[n]obody doubt[ed] . . . would constitute a concrete and particularized injury," the court turned to analysis of whether the defendants, through their alleged negligence, caused the plaintiffs a "substantial risk of identity theft."[107] The court found such a substantial risk through the plaintiffs' allegations of either financial fraud or healthcare fraud.[108] First, the exposure of Social Security numbers and credit card numbers alone constituted sufficient injury in fact with respect to financial fraud.[109] Second, and perhaps more interesting, the court found that the loss of personal information, as a combination of data, was sufficiently pled as to risk "medical identity theft."[110] In granting standing for either set of allegations, the court concluded that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."[111]

2. Narrow Theories

By contrast, the First, Second, Fourth, and Eighth Circuits have generally denied standing to data breach plaintiffs based on a future harm theory.[112] These circuits agree that the risk of potential injury is too speculative to survive an Article III analysis.[113] Part III of this Note examines the specific distinguishing characteristics of each of the leading cases in narrow jurisdictions.[114] But the Eighth Circuit's analysis in *In re SuperValu* illustrates the rationale underlying courts' choices to block standing for plaintiffs in data breach litigation actions.[115]

In 2014, the defendant supermarket announced that hackers had infiltrated its computer system and had gained access to stored customer financial information.[116] The

---

[107] *Id.*

[108] *See id.* at 628.

[109] *See id.*

[110] *See id.*

[111] *Id.* at 629.

[112] *See generally In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012). It must be noted here that prior to the Court's opinion in Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), the Third Circuit fell into this analysis pool. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 41–42 (3d Cir. 2011). Post-*Spokeo*, the Third Circuit may still retain its restrictive theory of standing for state law claims. *Accord* Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 91 (2017).

[113] *See In re SuperValu*, 870 F.3d at 767, 770–72; *Whalen*, 689 F. App'x at 90 (holding that the plaintiffs' canceled credit card and lack of additional lost personal information foreclosed risk of future injury); *Beck*, 848 F.3d at 275–76 (holding that a thirty-three percent chance of identity theft fell short of a "'substantial risk' of harm"); *Katz*, 672 F.3d at 80 (holding that the risk of future harm was insufficient to give the plaintiff standing without an actual unauthorized access).

[114] *See infra* Part III.

[115] *See generally In re SuperValu*, 870 F.3d 763.

[116] *Id.* at 766.

plaintiffs alleged both that they were exposed to a future risk of identity theft and that they had spent time and effort ensuring their potentially compromised information was not used to make fraudulent charges.[117] Despite acknowledging that third-party criminals did indeed steal the plaintiffs' financial data, the court declined standing to plaintiffs who had not alleged actual misuse of that data.[118] Because only the plaintiffs' financial data, and no "personally identifying information, such as social security numbers, birth dates, or driver's license numbers" were stolen, the plaintiffs could not—by their own evidence[119]—establish a substantial risk of future financial fraud.[120] Therefore, because the risk of future fraud theory was not "personal and individual" to these plaintiffs[121]—that they only established that a breach could result in fraud, not that they were at risk—time and effort spent to curtail the potential injury was unreasonable in response to the unsubstantiated threat.[122]

Both the Eighth and Second Circuit decisions tend to show the narrow-theory courts' unwillingness to find a credible risk of injury where hackers do not have the ability to utilize the data that was stolen.[123] The Fourth and First Circuits similarly failed to find a future harm injury without evidence of a data breach by theft, implying that a risk of identity theft or fraud is only feasible when a third party retrieves the data with ill-will and the intent to use it.[124] All narrow circuits therefore found a risk of future harm injury theory too speculative on the facts presented, but none of the circuits actually foreclosed risk of future harm as a valid Article III injury for data breach cases. Rather, the courts leave open the possibility that proper contextualization might sufficiently lower the courts' shield against suits involving generalized injuries—that a risk of future harm is never too speculative in data breach situations.

---

[117] *Id.* at 766–67.

[118] *Id.* at 769–70.

[119] *Id.* at 770–71 ("As the [Government Accountability Office (GAO)] report points out, compromised credit or debit card information . . . 'generally cannot be used alone to open unauthorized new accounts.' . . . [Also], the findings of the GAO report do not plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud." (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 30 (June 2007), https://www.gao.gov/assets/270/262899.pdf)).

[120] *See id.* (citing Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017)).

[121] *See id.* at 770 (citing and quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016)).

[122] *See id.* at 771; *cf.* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013).

[123] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017); *In re SuperValu*, 870 F.3d at 771 (explaining the inadequacy of the government report which stated there was minimal chance of fraud following a breach and there existed a lack of long-term study results to prove otherwise); *see also* Wynhausen, *supra* note 12, at 316 ("[The Eighth Circuit] effectively shut the door on any recovery for plaintiffs unless they can prove actual identity theft.").

[124] *See Beck*, 848 F.3d at 274 (remarking that no evidence had yet surfaced that a stolen laptop's contents had been accessed or misused or that a thief intended to steal plaintiffs' information when taking the device); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (denying plaintiff's risk of harm injury theory because there had yet been no breach).

III. STITCHING TOGETHER THE SPLIT CIRCUIT

Although the Courts of Appeal appear to have a binary divide between granting and denying Article III standing to data breach victims, upon closer examination, the circuit split is much more nuanced and potentially not a true split after all. For example, despite rulings on opposite sides of the "heightened risk" question, the circuits tend to agree that for instances of actual fraud or identity theft, costs borne to mitigate or prevent the effects of fraud and identity theft are actionable against defendants who have exposed the compromised data.[125] Further still, it is generally suggested that certain data types (e.g., financial information, critical records, and health histories), especially in combination with one another, tend to require a looser interpretation of standing to allow victimized plaintiffs an opportunity to recover.[126]

But in every case, the court seems to either allow or leaves open the question whether the data breach alone gives rise to the concrete, particularized, imminent injury required by Article III.[127] In the expansive theory jurisdictions, this notion is rather plain. The Seventh Circuit, for example, noted that once data has been stolen, "[i]t is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is 'sooner or later[ ] to make fraudulent charges or assume those consumers' identities[.]'"[128]

It follows from this reasoning that a future risk injury is intertwined with the data breach event. Put another way, when a hacker invades a digital system which stores sensitive data (or a garden variety thief steals an analogous physical device), that event is a data breach and it creates a liability for the party hosting that data because, "Why else would hackers break into a store's database and steal consumers' private information?"[129] Narrow theory jurisdictions tend to require plaintiffs to prove that thieves have put the figurative pen to paper, but these courts fail to appreciate "that an individual whose personally identifying information has been stolen and is subsequently in the hands of thieves or skilled hackers is far more at risk than someone whose data is still secure."[130] It is a fundamental misunderstanding in the narrow theory jurisdictions

---

[125] *See, e.g.*, *In re SuperValu*, 870 F.3d at 770 ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury." (quoting Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018))); *see also* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (finding that although fraudulent charges were not borne by the plaintiffs, other mitigation costs such as time spent monitoring and reviewing were sufficient injuries); *Whalen*, 689 F. App'x at 91 n.1 (contrasting the instant action with *Lewert*, suggesting that the instant plaintiff failed where the *Lewert* plaintiffs might have succeeded in the Second Circuit).

[126] *See, e.g.*, *Attias*, 865 F.3d at 628; *Whalen*, 689 F. App'x at 90–91.

[127] *See supra* Section II.B.

[128] *Lewert*, 819 F.3d at 967 (alteration in original) (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).

[129] *See Remijas*, 794 F.3d at 693.

[130] Kimberly Fasking, Comment, Beck v. McDonald*: The Waiting Game—Is an Increased Risk of Future Identity Theft an Injury-in-Fact for Article III Standing?*, 41 AM. J. TRIAL ADVOC. 387, 402 (2017).

that loss of consumer data is not an injury to the consumer. Fortunately, these courts have not entirely foreclosed that these data breach victims are without recourse—rather, each circuit's jurisprudence tends to show the courts' willingness to grant standing to these plaintiffs if their risk of future harm is properly contextualized.[131]

Therefore, a simple circuit split solution follows: a data breach alone is sufficient to survive the injury in fact analysis. The expansive theory jurisdictions, in addition to the Seventh Circuit, provide support for this approach.[132] Indeed, the Ninth Circuit goes further than the D.C. and Sixth Circuits by explicitly rejecting defendants' claims that a threat of identity fraud was no longer imminent at the time of litigation.[133] In doing so, the necessary implication is that once data has been stolen, the threat to victims is permanent.[134] Therefore, plaintiffs should achieve, and continually possess, standing in actions against data breach defendants from the moment of the breach onward. Though other standing frameworks may be foreclosed in narrow jurisdictions, the following analysis supports that each circuit's approach is readily compatible with the "breach alone" concept.

A. First Circuit

The First Circuit adjudicated its most recent data breach litigation case in 2012.[135] Because *Katz* was decided pre-*Clapper*, even considering the court's then-narrow approach, the question of whether a data breach alone may satisfy the court's standing requirements bears less scrutiny than in sister circuits. In this case, the plaintiff alleged that her sensitive information was improperly stored by defendant and left unprotected from potential unauthorized access.[136] The plaintiff did not allege any actual theft of the data; therefore, the court found no standing to sue for the threat of theft.[137] But the court itself distinguished its ruling from cases where

---

[131] *See infra* notes 132–59 and accompanying text.

[132] *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) ("[A]n unauthorized party has already accessed [the] data . . . and it is much less speculative . . . to infer that this party has both the intent and the ability to use that data for ill."); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("There is no need for speculation where [p]laintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals.").

[133] *See In re* Zappos.com, Inc., 888 F.3d 1020, 1028 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

[134] *See* 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/ [https://perma.cc/62WG-TYLN].

[135] *See generally* Katz v. Pershing, L.L.C., 672 F.3d 64 (1st Cir. 2012).

[136] *See id.* at 70.

[137] *See id.* at 79.

data is "actually . . . accessed by one or more unauthorized third parties."[138] By its own language, First Circuit jurisprudence appears to neatly settle within a breach alone approach.

B. Second Circuit

In *Whalen v. Michaels Stores, Inc.*, the Second Circuit declined standing to a litigant who was not only impacted by a data breach, but also fell victim to attempted fraudulent purchases through the stolen data.[139] Because the plaintiff had promptly cancelled her credit card after the fraudulent purchases, the court did not accept the plaintiff's theory of future risk of harm.[140] The court further implied that had the breach included additional sensitive information, the threat of identity fraud would present a stronger argument.[141]

The court's rationale relies on a fundamental misunderstanding of modern identity theft tactics.[142] Potential thieves need as little as one piece of information to successfully steal a victim's identity.[143] Even an exposed credit card number might reveal enough information to continue an identity theft scheme long after the cardholder cancels the card.[144] The court cited both Sixth and Seventh Circuit opinions to contrast the *Whalen* plaintiff's insufficiency with, plausibly, cases it presumes are correctly decided.[145] With proper framing regarding the reach of identity theft, the Second Circuit may likely reverse course and adopt the breach alone approach.[146]

---

[138] *See id.* at 80.

[139] 689 F. App'x 89, 90 (2d Cir. 2017).

[140] *Id.*

[141] *Id.* at 90–91.

[142] *See id.* It is also of import that the *Whalen* opinion was issued as a summary order and is limited in both its analysis and its reliance on case law. The Second Circuit has yet to render a precedential opinion discussing data breach litigants' standing.

[143] *See* Lisa Rogak, *10 Things You Should Know About Identity Theft*, CREDITCARDS.COM, https://www.creditcards.com/credit-card-news/help/10-things-you-should-know-about-identity-theft-6000/ [https://perma.cc/5QQD-78RM] (last visited Mar. 15, 2021) (discussing how even nonfinancial personal information, such as email login credentials or a telephone number, can be enough for a thief to steal someone's identity). *See generally* Will Kenton, *Social Engineering*, INVESTOPEDIA (May 10, 2019), https://www.investopedia.com/terms/s/social-engineering.asp [https://perma.cc/64CZ-PATM] (describing a common method of accessing sensitive pieces of information to fraudulently create an identity package of another person).

[144] *See* Rogak, *supra* note 143, § 10 (noting that major credit bureaus provide free credit monitoring for up to ninety days, contradicting the *Whalen* court's assertion that identity fraud threats cease upon card termination).

[145] *See Whalen*, 689 F. App'x at 90 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016)); *id.* at 91 n.1 (citing Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., L.L.C., 794 F.3d 688 (7th Cir. 2015)).

[146] *But see Whalen*, 689 F. App'x at 90. The court rejected one of the plaintiff's harm theories

C. Fourth Circuit

In 2013, a laptop containing sensitive healthcare data was determined to have been stolen from a hospital.[147] The Fourth Circuit denied standing to affected patients who sued on a risk of health identity theft theory.[148] The court specifically distinguished this theory as presented from Seventh Circuit precedent based on the *Beck* plaintiffs' failure to allege that an unauthorized third party sought out the laptop to infiltrate it for the purpose of stealing the sensitive data.[149] The court also noted that the missing laptop was never found, and the plaintiffs could not show that the sensitive data was ever accessed.[150] Despite defendant's own investigation concluding that the laptop had been stolen,[151] the court concluded that the chain of attenuation between theft and the alleged potential harm was too speculative post-*Clapper*.[152]

Further, the court rejected the plaintiffs' argument that they also suffered a substantially increased risk of future harm.[153] Though the plaintiffs had provided evidence "that 33% of those affected by [defendant's] data breaches will become victims of identity theft,"[154] the court declined to find this increased risk—presumably from zero risk to a one-in-three chance—substantial.[155] But like the Second Circuit in *Whalen*, the Fourth Circuit relied on an incomplete understanding of the gravity of lost or stolen data.[156] Due to certain data's critical—and potentially perpetual[157]—nature,

based on actual fraudulent purchases with the stolen data, because although fraudulent purchases were attempted, the plaintiff was never required to pay for them. *Id.*

147 Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).

148 *Id.* at 274.

149 *See id.*

150 *See id.*

151 *Id.* at 275.

152 *See id.* (noting that the plaintiffs' arguments relied on thieves both targeting the laptop to steal identities and then choosing the named plaintiffs to defraud—neither of which were alleged or proven).

153 *Id.*

154 *Id.* at 276.

155 *See id.* In footnote, the court also discarded the plaintiffs' allegation that "data-breach victims are 9.5 times more likely than the average person to suffer identity theft" because that statistic spoke to breaches generally rather than to the litigated breach. *See id.* at 275 n.7.

156 *See supra* notes 132–34 and accompanying text.

157 For example, state law requires retention of medical records by medical doctors and hospitals for various lengths of time, but generally for five to ten years following the patient's last treatment or visit. *See* Kristina Ericksen, *How Long Are Medical Records Kept? And 9 Other Health History FAQs*, RASMUSSEN COLL. (Aug. 15, 2017), https://www.rasmussen.edu/degrees/health-sciences/blog/how-long-are-medical-records-kept/ [https://perma.cc/YE8Z-E96S]; *see also* Joy Pritts et al., *Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Medical Record Access Laws*, AGENCY FOR HEALTHCARE RSCH. & QUALITY, Appx. A-7 (Aug. 2009) (surveying state medical record retention requirements for hospitals and doctors); *cf.* MASS. GEN. LAWS ch. 111, § 70 (2008) (requiring a twenty-year holding period for medical records). But do these laws apply to technology

risk of identity theft can be ever-present.[158] Given adequate contextualization and fact-framing, courts like the Fourth Circuit may be more willing to ease their apprehensions about abstract theories of harm.[159] Like the Eighth Circuit, it appears that evidentiary quality would be a tipping point towards granting standing should the Fourth Circuit be confronted with the "breach alone" theory.[160]

D. Eighth Circuit

The essential facts of *SuperValu* are discussed *supra* in Section II.B.2. Although the Eighth Circuit denied these plaintiffs standing based on a risk of future harm theory, the court also noted that the insufficiency of the evidence proffered to support the theory was the fatal flaw in the allegation.[161] The plaintiffs' reliance on a then decade-old federal report failed to adequately support their argument that data breaches often result in identity theft to victims.[162] Because the plaintiffs' evidence did not show that their stolen financial data would (by itself) likely be used fraudulently, plaintiffs could not prove a substantial risk of future harm.[163]

---

companies like Google, with whom healthcare providers share patient information? *See* Natasha Singer & Daisuke Wakabayashi, *Google to Store and Analyze Millions of Health Records*, N.Y. TIMES (Nov. 11, 2019), https://www.nytimes.com/2019/11/11/business/google-ascension-health-data.html [https://perma.cc/ZG92-TKNC]. If not, patient health records—and a risk of identity theft—may exist for many decades—as long as Google's servers keep running.

[158] *See* Sid Kirchheimer, *Protecting the Dead from Identity Theft*, AARP BULL., https://www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html [https://perma.cc/7UBE-ULCB] (last visited Mar. 15, 2021) (discussing how even the deceased can be targets of identity theft).

[159] For healthcare data breaches especially, the risk of "general" identity theft appears to be much more substantial than the *Beck* plaintiffs alleged with respect to health identity theft. *See* Jessica Davis, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTHITSECURITY (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud [https://perma.cc/XC67-JZMK] (noting a recent study that found 150 million patients' "Social Security numbers, dates of birth, [and/or] driver's licenses [sic] numbers" were exposed in 194 healthcare data breaches); *cf.* Steven Bearak, Opinion, *Medical Identity Theft on the Rise—5 Tips to Protect Your Employees and Clients*, SC MEDIA (May 23, 2017), https://www.scmagazine.com/home/opinion/executive-insight/medical-identity-theft-on-the-rise-5-tips-to-protect-your-employees-and-clients/ [https://perma.cc/5DHV-B7F5] (noting that "medical identities are 20 to 50 times more valuable to criminals than financial identities").

[160] *See supra* Section II.B.2; *infra* Section III.D.

[161] *See In re* SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017) ("It is possible that some years later there may be more detailed factual support for plaintiffs' allegations of future injury. But such support is absent from the complaint here . . . .").

[162] *Id.* ("The 2007 [GAO Report] found that '[c]omprehensive information on the outcomes of data breaches is not available,' and the 'extent to which data breaches result in identity theft is not well known[.]'" (citations omitted)).

[163] *See id.* at 770–71.

However, in footnote, the court recognized without "comment[ing] on the sufficiency," that the plaintiffs likely had other avenues to prove a risk of future harm theory.[164] The court also specifically noted that the plaintiffs failed to advance a "breach alone"–style argument on appeal.[165] Simply put, the Eighth Circuit did not actually foreclose the "breach alone" approach, and might likely adopt it given adequate evidentiary support.

IV. PROPOSED DATA BREACH STANDING FRAMEWORKS

A. Unpacking the "Breach Alone" Approach

The preceding circuit split analysis focused on identifying a clear, plausible thread of continuity among all of the circuits to establish that data breach litigants should ideally enjoy Article III standing perpetually beginning at the moment of breach.[166] The "breach alone" approach simply asks whether a data breach has occurred. If so, a litigant successfully proves an injury in fact. However, it is not difficult to recognize that the "breach alone" analytical framework is not necessarily a clean solution for data breach litigants. Indeed, if the *amici curiae* briefs filed by the technology giants in *Spokeo* are any indication, corporations against whom liability would be imposed in data breach suits may be, logically, vigorously opposed to allowing litigants standing to sue in any situation.[167]

---

[164] *Id.* at 771 n.5.

[165] *See id.* (noting that the district court discussed whether the data breach constituted a cognizable "invasion of privacy" and that the "plaintiffs [did] not press [the argument] on appeal").

[166] *See supra* Part III.

[167] *See, e.g.*, Brief for Experian Information Solutions, Inc. as Amicus Curiae Supporting Petitioner at 8, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) ("Indeed this very case is an example of a class action concerning no concrete harm."); *see also* Brief for Amici Curiae eBay Inc., Facebook, Inc., Google Inc., and Yahoo! Inc. in Support of Petitioner at 1–7, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) [hereinafter Facebook Amicus]. *See generally* David J. Baldwin, Jennifer Penberthy Buckley & Ryan Slaugh, *Insuring Against Privacy Claims Following a Data Breach*, 122 PENN STATE L. REV. 683 (2018) (identifying commonly litigated issues in data breach trials and options for companies to protect against potential liability). Some major corporations have recently jumped onto the consumer data privacy bandwagon. *See, e.g.*, YouTube Commercials, *Privacy on iPhone—Simple as That—Apple*, YOUTUBE (July 28, 2020), https://www.youtube.com/watch?v=lHcf9ZkJ28o ("Right now, there is more private information on your phone than in your home. Think about that—so many details about your life, right in your pocket. This makes privacy more important now than ever. Your location, your messages, your heartrate after a run—these are *private* things—*personal* things. And they should belong to you. Simple as that." (emphasis added)). It is unclear whether these corporations would also advocate to grant standing to data breach plaintiffs, their push for consumer data privacy notwithstanding. *Compare* Facebook Amicus (filed with the Court

If a breach occurs and a victim has not yet suffered an identity fraud, has no expenses related to, for example, credit monitoring, or related costs have already been reimbursed by the breached entity, what damages can a court reasonably assess?[168] It is true that damages in future risk of harm cases are necessarily somewhat imprecise;[169] however, an imprecise damages calculation does not translate to zero liability. Plaintiffs need not prove a dollar amount of damages to secure a favorable judgment.[170] Further, the "breach alone" approach relates specifically to the injury in fact prong of Article III standing analysis—redressability is an interrelated but separate issue. Data breach litigants' path forward after proving an injury in fact is beyond the scope of this Note.

Another potential criticism is the question of who is truly responsible for a data breach. Which entity or individual should litigants target for recovery in data breach actions?[171] For example, when data resides in the cloud, there are at least three vulnerability points which hackers could target: (1) the customers (the typical data breach suit plaintiffs); (2) the data owners (the typical defendant in these actions [e.g., CareFirst, Michaels Stores, etc.]); and (3) the data holders (the entity running the data-hosting servers [e.g., Amazon Web Services]).[172] If hackers infiltrate a security system and steal identifying customer data, should those users who are now

---

in 2014), *with* Julia Carrie Wong, *Facebook's Zuckerberg Announces Privacy Overhaul: 'We Don't Have the Strongest Reputation*,*'* GUARDIAN (Apr. 30, 2019, 3:52 PM), https://www.theguardian.com/technology/2019/apr/30/facebook-f8-conference-privacy-mark-zuckerberg [https://perma.cc/E8UJ-FJYA] (reporting that the founder of Facebook intended to gear the site towards becoming a "privacy-focused social platform").

[168] *See* Dowty, *supra* note 12, at 702–04.

[169] *Id.* at 702 ("[C]ourts first have to speculate as to whether theft or fraud might happen, and then, speculating that it will happen, speculate further as to what potential damages might result.").

[170] *See* Eric S. Boos, Chandler Givens & Nick Larry, *Damages Theories in Data Breach Litigation*, 16 SEDONA CONF. J. 125, 146–47 (2015) (noting that under privacy statutes, plaintiffs need not prove financial harm); Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. BAR J. 30, July–Aug. 2016, at 35 (noting a successful use of data breach litigants' unjust enrichment theory).

[171] *See Who Is Liable When a Data Breach Occurs?*, THOMSON REUTERS: LEGAL, https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability [https://perma.cc/AY2A-5257] (last visited Mar. 15, 2021).

[172] *Id.* Note that the second and third types of vulnerability points can coincide when the owner of the data hosts its own server system like Google. *See generally Data and Security*, GOOGLE DATA CTRS., https://www.google.com/about/datacenters/data-security/ [https://perma.cc/6M6Q-UBXE] (last visited Mar. 15, 2021). In its Privacy and Security Compliance FAQ, Google states, "Your data [is] stored in Google's network of data centers." *Compliance*, GOOGLE CLOUD HELP, https://support.google.com/googlecloud/answer/6056694 [https://perma.cc/EDD6-L6FZ] (last visited Mar. 15, 2021).

susceptible to identity theft seek recovery from the data owner or the data host?[173]—both?[174]—neither?[175] However, the appropriate question for the injury in fact inquiry is "was there harm," not "who caused the harm." Therefore, the investigation into the ultimately responsible party is better suited to the nexus prong of the constitutional standing analysis, not the injury in fact prong, and is correspondingly also outside the scope of this Note.

Despite properly allocating some potential criticisms to the appropriate portions of Article III standing analysis, the "breach alone" framework is perhaps too heavy of a sword for data breach plaintiffs to wield. In effect, any data breach would trigger strict liability on the part of a data owner or host, which simply has the potential to go too far.[176] "Big data" has some positive social benefits,[177] and imposing presumably

---

[173] *See generally Data Breach Response: A Guide for Business*, FED. TRADE COMM'N (May 2019), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf [https://perma.cc/SH8J-JZS6]. The Federal Trade Commission suggests that the onus is on the data owner to ensure a data host operates with good security practices, *see id.* at 3, but in the event of a breach, data hosts are likely required to notify the data owners, *id.* at 6, implying potential ultimate liability. Of course, data owners also might owe notice to consumers. *See id.* at 6–9.

[174] *See* Edward J. McAndrew, *Surviving the Service Provider Data Breach*, DLA PIPER (July 29, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/07/surviving-the-service-provider-data-breach/ [https://perma.cc/X7VR-ALN5] ("Covered entities and their service providers are ending up as co-defendants in data breach class action litigation," where, analogous to terms used here, a covered entity is equivalent to a data owner and a service provider is equivalent to a data host.).

[175] *See* Kayla Matthews, *Who's Financially Responsible for Cybersecurity Breaches?*, SEC. BOULEVARD (Sept. 17, 2019), https://securityboulevard.com/2019/09/whos-financially-responsible-for-cybersecurity-breaches/ [https://perma.cc/99CQ-CCQB] (noting existing argument that customers "vote with their wallets" to support only companies with the best consumer protections).

[176] *See* Seth D. Rothman & Dennis S. Klein, *Defending a Data Breach Class Action*, LEGAL INTELLIGENCER, June 6, 2016, at 4, 4 (highlighting the recent trend of "data breach[] . . . litigation" and surveying certain "high-profile settlements" as viable, if not preferable options to trial); *cf.* Facebook Amicus, *supra* note 167, at 12–15 (arguing that standing must protect defendants from the threat of litigation based on statutory procedural violations). *But see, e.g.*, Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 627 (2018) (drawing on the common law development of products liability to sketch a framework for a data breach-specific tort); Colin J.A. Oldberg, Note, *Organizational Doxing: Disaster on the Doorstep*, 15 COLO. TECH. L.J. 181, 199–205 (2016) (advancing strict liability as the preferable framework in data breach cases involving hacking and doxing because it would force entities to "beef up security, or risk going out of business").

[177] Daniel Riedel, *The Duality of Big Data: The Angel and the Demon*, WIRED (Oct. 2014), https://www.wired.com/insights/2014/10/duality-big-data/ [https://perma.cc/P7ZJ-E69D] (discussing how "big data" is utilized to provide services that help improve societies in areas such as healthcare and environmentalism).

large fines and judgments on data owners (and holders) for these data breaches may net negative if the entities are forced out of business.[178] Therefore, two slightly narrower alternative solutions are proposed in addition to the broadest "breach alone" framework to mitigate concerns of overreach. This Note ultimately recommends that the Court adopts the latter approach to achieve the proper balance of Article III sword and shield.

B. "Piggybacking" Approach

Similar to the class action device,[179] the "piggybacking" approach would utilize the injury to one plaintiff to establish sufficient injury for another plaintiff.[180] However, "piggybacking" would act like a reverse class device. Where named plaintiffs of a class action cannot draw on harms to other unnamed plaintiffs to establish injury in fact,[181] "piggybacking" would utilize the Article III–sufficient injury of an unnamed data breach victim to establish an imminent, concrete, particularized risk of future harm for the instant, named data breach plaintiff.[182]

Although practically the narrowest of the three advanced proposals, "piggybacking" would require perhaps the most radical overhaul of the Court's prudential standing doctrine. This approach would borrow significantly from the concept of *jus tertii*: "third party rights."[183] Under modern jurisprudence, as a means of prudential self-limitation, the Court has in place a generalized bar on litigants asserting the rights of a third

---

[178] *Cf.* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 980–82 (2016) (arguing that negligence standards appropriately weigh economic benefits of credit card systems against transaction costs).

[179] 7A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1751 (3d ed. 2020) ("[T]he class action [is] a procedural device for resolving disputes affecting numerous people.").

[180] *See In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017) ("A putative class action can proceed as long as one named plaintiff has standing."). The underlying procedural mechanics of establishing a class are not helpful to expand on "piggybacking"; therefore, class actions are merely referenced without further procedural analysis.

[181] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 634 (3d Cir. 2017) (citing Lewis v. Casey, 518 U.S. 343, 357 (1996)).

[182] This approach is distinguished from the general class action bar against achieving standing through harms to unnamed plaintiffs, *see Lewis*, 518 U.S. at 357 (citing Simon v. E. Ky. Welfare Rts. Org., 426 U.S. 26, 40 n.20 (1976)), because the "piggybacking" plaintiff would show a risk of future harm injury through the actual identity theft or fraud of other victims of the same data breach. *Cf. id.* at 395–96 (Souter, J., dissenting in part) (Once the named class action plaintiff's standing fails mid-litigation, "even then the question is not whether suit can proceed on the standing of some unnamed members of the class, but whether 'the named representative [can continue] to "fairly and adequately protect the interests of the class."'" (quoting Sosna v. Iowa, 419 U.S. 393, 403 (1975))).

[183] *See* Brian Charles Lea, *The Merits of Third-Party Standing*, 24 WM. & MARY BILL RTS. J. 277, 299–302 (2015) (providing a brief overview of *jus tertii*'s origin and application over time).

party.[184] But like all judicial fabrications, that prohibition is both malleable and with gaping exception, exemplified by *jus tertii*.[185]

Modern *jus tertii* doctrine allows a third party to vindicate the rights of an injured party when that third party shares a close relationship to the victim and the victim faces some obstacle to redressing that injury him- or herself.[186] The "piggybacking" approach advanced here would borrow the first prong from *jus tertii* doctrine and flip the second prong on its head. The third party under this framework will have still suffered some clear injury—an identity theft or fraud—and the "piggybacker" must sufficiently prove that injury with respect to the third party—i.e., the "piggybacker" would simply prove the "unnamed" third party suffered the injury. However, the nexus between the third party and the "piggybacker" need only exist to the extent that both individuals were victims of the same breach. In effect, the "piggybacker" shows a substantial risk of fraud or identity theft through the *actual* fraud or identity theft of a victim of the same data breach instance—a type of injury that would be recognized by each of the split circuits.[187]

The "piggybacking" approach would shrink the data breach plaintiff's sword considerably (compared to the "breach alone" approach). But its origins in both the class action device and *jus tertii* theory open this approach to vast criticism.[188] *Jus tertii* is not only an exception to standing but an exceedingly narrow exception.[189] Similarly, class actions require a host of hoops to jump through for certification and have largely fallen out of favor with courts.[190] Despite providing a more generous shield to the courts (and potential data breach litigation defendants alike), this approach would likely remain nonviable.

C. "Tiered Sensitivity" Approach

Recognizing the potentially radical effect of the "piggybacking" framework and the broad (and, therefore, potentially too plaintiff-friendly) "breach alone" framework,

---

[184] *See id.* at 296.

[185] *See id.* at 298 (noting *jus tertii* as a major exception to prudential standing).

[186] *Id.* at 300–01 (further noting the Court's relaxed application of both *jus tertii* prongs).

[187] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016). *But see* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017). In *Whalen*, the court denied injury in fact based on, among other theories, fraudulent purchases because the plaintiff had not been asked to pay for any of the false charges. *Id.* However, the court erred in its ruling based on a misunderstanding of modern identity theft. *See supra* Section III.B.

[188] *See generally* Linda S. Mullenix, *Ending Class Actions as We Know Them: Rethinking the American Class Action*, 64 EMORY L.J. 399, 406–17 (2014) (overviewing both positive and negative critiques of the class device).

[189] *See* 16 C.J.S. CONSTITUTIONAL LAW § 167 (2020).

[190] *See* Robert H. Klonoff, *The Decline of Class Actions*, 90 WASH. U. L. REV. 729, 731 (2013).

this Note recommends an approach that splits the differences in the two concepts to avoid holstering litigants' swords or confiscating the judiciary's shield entirely. Most of the circuits analyzed in this Note recognize the highly sensitive nature of the data that litigants address in their breach litigation.[191] Some courts go further to identify which types of data are worthy of more rigid scrutiny when exposed to third party theft by breach defendants.[192]

Similarly, common sense tells us that a telephone number is not as intrinsically linked to the individual as is a single Social Security number assigned throughout the lifetime of the individual.[193] Therefore, a compromise approach in data breach litigation must account for tiers of data sensitivity, analyzed more severely as sensitivity increases. This approach would parallel the Court's existing standards of review in Equal Protection Clause inquiries,[194] recognizing that some classes of data may require a rebuttable presumption of imminent identity theft or fraud,[195] while others ask more of plaintiffs to prove the same.[196]

The most critical, intrinsic data types, for example, vital health records and Social Security numbers,[197] would receive "strict scrutiny," or the highest level sensitivity analysis.[198] In this tier, because the breached data has such value to hackers even in

---

[191] *See, e.g.*, *Whalen*, 689 F. App'x at 90–91; Attias v. CareFirst, Inc., 865 F.3d 620, 627–28 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); *In re SuperValu*, 870 F.3d at 770–71.

[192] *See, e.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1027–29 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019); *In re SuperValu*, 870 F.3d at 770–71.

[193] *See Do You Need a New Social Security Number?*, FED. TRADE COMM'N (July 2012), https://www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number [https://perma.cc/CK6Y-LPZE] (outlining extreme, rare examples for requesting a new Social Security number).

[194] *See* Eric Heinze, *The Logic of Standards of Review in Constitutional Cases: A Deontic Analysis*, 28 VT. L. REV. 121, 129 (2003) ("The Supreme Court has adopted three general standards of review in constitutional cases: 'strict scrutiny,' '[intermediate] scrutiny,' and 'rational basis review.'").

[195] *See* 16B C.J.S. CONSTITUTIONAL LAW § 1275 (2020) (defining the test for strict scrutiny).

[196] *See id.* §§ 1278–79 (defining the tests for intermediate scrutiny and rational basis).

[197] *See* Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[198] *See* 16B C.J.S. CONSTITUTIONAL LAW § 1275. When discussing the importance of protecting PII, the federal government recognized that some data, including Social Security numbers, "are particularly sensitive and may alone present an increased risk of harm to the individual." OFF. OF MGMT. & BUDGET, *supra* note 77, at 22. Indeed, the U.S. Department of Homeland Security (DHS) delineates two tiers of PII, where Sensitive PII (SPII) carries strict handling protocols due to its "increased risk to an individual if the data are compromised." *See* U.S. DEP'T OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION 3–6 (2012), https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII_0.pdf [https://perma.cc/XZ4A-F668]. DHS's SPII categories include both stand-alone data, like Social Security numbers, and data that becomes sensitive when paired with general PII—i.e., "medical information" paired with an email address. *Id.* at 5.

isolation,[199] the presumption would be that hackers will imminently harm the plaintiff, and the burden would fall to the defendant to prove substantial non-imminence or some other substantially countervailing affirmative defense—loosely related to compelling interest and narrow fit.[200]

Slightly less sensitive but still significant data, for example, financial information, would receive "intermediate scrutiny."[201] In this tier, the same presumption of imminent threat of future harm would still exist, but the defense need only prove by a preponderance of facts that the threat is not imminent or that it has a countervailing reason to be held harmless—paralleling the important government objective requirement.[202]

The least sensitive data, for example, telephone numbers and email addresses, would be analyzed similarly to the "rational basis test," or the lowest level of scrutiny.[203] In this tier, the presumption of imminent future harm would be stricken because the types of data within this tier would not fall within a "suspect class" due to its general, isolated lack of value to hackers.[204] Defendants would therefore only have to prove non-imminence (or some other attack on injury in fact) if the plaintiffs could rebut the lack of presumption—essentially the "presumption" rests with the defendant, correlating to a rational basis.[205]

This framework would also lend itself to modification if—and more likely when[206]—a data breach encompasses multiple types of data across the scrutiny tiers (e.g., both telephone and Social Security numbers). A court would have three options to proceed: (1) analyze each claim under its appropriate tier, likely, for example, invalidating the rational basis data claims and allowing suit for the strict scrutiny data; (2) developing additional scrutiny tiers to accommodate the blended tier claims; or (3) analyzing the combination of data loss across tiers as simply more severe than data lost within a tier. This Note recommends the third option because, as the federal government has noted, some information may alone not be utilized for identity theft, but in combination with other data, a data breach victim can more easily become the victim of identity theft.[207]

Many of the same vulnerabilities of the "breach alone" and "piggybacking" approaches apply to the "tiered sensitivity" approach. However, the "tiered sensitivity" approach presents a neat compromise position that seems to answer most prior criticisms.[208] In particular, tiering data by level of intrinsic value to the victim affords

---

[199] *See* Weisbaum, *supra* note 9.

[200] *See* 16B C.J.S. CONSTITUTIONAL LAW § 1275.

[201] *See id.* § 1278.

[202] *See id.*

[203] *See id.* § 1279.

[204] *See id.* §§ 1275, 78–79; *see also* Weisbaum, *supra* note 9.

[205] *See* 16B C.J.S. CONSTITUTIONAL LAW § 1279.

[206] *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) (where the breached data included, inter alia, "email addresses, social security numbers, and credit card information").

[207] *See* OFF. OF MGMT. & BUDGET, *supra* note 77, at 8, 22.

[208] *See supra* notes 168–78, 185–87 and accompanying text.

the most fairness to both plaintiffs and defendants, because the most vulnerable plaintiffs have the highest chance to be vindicated at trial, but not every data breach defendant will have to expend resources for the same given particular criteria. In short, the "tiered sensitivity" approach recognizes the reality and value of what is lost in data breaches, but balances victims' swords against the necessity of shielding both defendants and courts from burdensome litigation over information unlikely to lead to harm.

V. SOCIETY IS MOVING TOWARDS DATA PROTECTION, AND THE COURT MUST FOLLOW SUIT

A. Non-Congressional Legislative Models Buttress the "Tiered Sensitivity" Model

Though Congress has yet failed to enact a broad, unified reform for data breach remediation, state and international legislatures have recently trended towards large-scale data protection regulations.[209] Justice Brandeis's laboratories of democracy idea[210] supports the argument that state and comparable foreign sovereigns serve as a social marker to inform and direct a federal framework of data protection, if not in Congress, then through the judiciary.

1. The General Data Protection Regulations (GDPR)

In 2016, the European Union adopted the GDPR as a vast data protection framework for its citizens.[211] The GDPR instills individuals with "fundamental" digital rights,[212] including a right of remedy against any "controller" or "processor" who fails to abide by its provisions.[213] One example GDPR provision requires notification to an individual when a controller or processor suffers a data breach.[214] Two important considerations flow from this provision.

---

[209] *See generally Data Protection Law: An Overview*, CONG. RSCH. SERV. (Mar. 25, 2019), https://fas.org/sgp/crs/misc/R45631.pdf [https://perma.cc/2D6Y-2DHR] (providing a summary of existing legislation in state, federal, and international jurisdictions).

[210] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

[211] *See generally* Council Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter EU GDPR], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/4MDA-YL3J].

[212] *See id.* at L 119/32, art. 1; *see also id.* at L 119/1 ("The protection . . . of personal data is a fundamental right.").

[213] *Id.* at L 119/81, art. 82; *see id.* at L 119/33, art. 4, recitals 7–8 (defining "controller" and "processor" broadly).

[214] *See id.* at L 119/52–53, art. 34; *see also id.* at L 119/17, recitals 86–88.

First, requiring data handlers to inform affected individuals of a data breach lends support to the "breach alone" and "tiered sensitivity" approaches.[215] Forcing disclosure to victims of a data breach implies that harm to the individual occurs at the moment of breach, not upon either a risk of potential harm or actual fraud or identity theft.[216]

Second, and perhaps most instructively, the GDPR also scales the notification requirement for handlers to the sensitivity of the stolen information and the severity of the breach.[217] Essentially, if the breached data is highly sensitive or affects the "rights and freedoms" of victims, the notification must be near-immediate, unless countervailing interests would suggest otherwise.[218] The GDPR's minimal scaling for requiring notification to affected data breach victims is a useful jumping off point for the Court to implement the "tiered sensitivity" framework, since it mirrors many of the attributes of the approach.

2. State-Level Approaches to Data Protection

In the face of congressional silence, many states have instituted frameworks of varying degree and scope to jumpstart the process of protecting users' data. The most robust of these is the California Consumer Privacy Act (CCPA), which imposes security and notification requirements on businesses meeting certain criteria.[219] Other states have waded and continue to wade into the waters of data privacy legislation, each with nuanced measures to illicit stronger data privacy considerations from both the custodians of data and the individual citizens (who may be potential litigants in data breach actions).[220]

---

[215] *Supra* Part III & Section IV.A ("breach alone"); Section IV.C ("tiered sensitivity").

[216] *See* EU GDPR, *supra* note 211, at L 119/17, recitals 86–88.

[217] *See id.* at L 119/52–53, art. 34; *see also id.* at L 119/17, recitals 86–88.

[218] *See id.* at L 119/52–53, art. 34; *see also id.* at L 119/17, recitals 86–88.

[219] *See* CAL. CIV. CODE § 1798.100 (West 2020). In the 2020 election, California voters passed the California Privacy Rights Act, which will expand and amend the CCPA, including its notification requirements. *See* Stacey Gray, Katelyn Ringrose, Polly Sanderson & Veronica Alex, *California's Prop 24, the "California Privacy Rights Act," Passed. What's Next?*, FUTURE PRIV. F., https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/ [https://perma.cc/C7TK-L4SA] (Dec. 17, 2020); *see also* Else Feikje van der Berg, *"CCPA 2.0" Could Significantly Expand the CCPA*, DATAWALLET (June 21, 2020, 10:00 PM), https://datawallet.com/blog/ccpa-2-0-could-significantly-expand-the-ccpa [https://perma.cc/7F97-R6BR] (providing an overview of the CPRA's key provisions).

[220] For a summary of recently enacted or pending data privacy legislation, see Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/45Q2-PQ7N] (last visited Mar. 15, 2021). The document is regularly updated to reflect legislative fluctuations.

Though it is promising that states have taken it upon themselves to introduce protective measures where the federal government has failed, the lack of uniformity across state lines is indicative of why the Court's resolution of the circuit split would be a welcome, and necessary, addition to data users' arsenal to recover for data breach losses. Importantly, in support of a cross-continental agreement on data protection standards, state legislation generally shares commonality with the GDPR with respect to notice requirements and private rights of action for victims of data breaches.[221] Therefore, domestic jurisdictions appear to be encouraging a unified front for protecting data breach victims, leaving open the opportunity for the Court to adopt a data breach-specific injury in fact constitutional standing framework as a complement to state efforts.

a. California

The CCPA implemented a framework of data protection for California citizens.[222] The CCPA requires businesses meeting certain criteria[223] to take "reasonable security procedures" to protect consumer data.[224] For individuals, the CCPA establishes a private right of action against qualifying businesses upon "unauthorized access and exfiltration, theft, or disclosure" of data.[225] Despite its scope to only California businesses and citizens, the CCPA is undoubtedly the most far-reaching state-level consumer-protective legislation in the United States to date.[226]

b. Nevada & Maine

Nevada's personal information protection framework includes for Nevada citizens a data breach notification provision.[227] However, it does not include a private right of action for typically affected individual victims.[228] Interestingly, the Nevada

---

[221] *See, e.g.*, CAL. CIV. CODE § 1798.150; An Act Relative to the Collection of Personal Information by Business, H.B. 1680, 2020 Sess. (N.H. 2020).

[222] *See* CAL. CIV. CODE § 1798.100.

[223] *Id.* § 1798.140 (defining "business" as any for-profit company operating in California that (1) has $25 million in gross annual revenue; (2) alone or in combination buys, sells, or shares personal data of 50,000 or more people; or (3) gets over half of its revenue from selling consumer data).

[224] *Id.* § 1798.150.

[225] *Id.* For a comparison of the CCPA to the GDPR, see *America's GDPR? Seven Workstreams to Implement California's Consumer Privacy Act*, PWC (2018), https://www.pwc.com/us/en/services/consulting/assets/pwc-americas-gdpr-seven-workstreams.pdf [https://perma.cc/UW7B-CMRM].

[226] *See* Greg Bensinger, *So Far, Under California's New Privacy Law, Firms Are Disclosing Too Little Data—Or Far Too Much*, WASH. POST (Jan. 21, 2020, 7:44 PM), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/ [https://perma.cc/P57N-42UC] ("The CCPA is considered the nation's most far-reaching online privacy law and a potential model for other states.").

[227] NEV. REV. STAT. ANN. § 603A.220 (West 2006).

[228] *See generally id.* §§ 603A.300–360.

notification requirement looks similar to the GDPR requirement, demanding an immediate notification to affected individuals unless there are countervailing interests to delay the notification.[229]

Maine's legislation is by far the least protective of the three state-enacted frameworks presented.[230] For Maine citizens, it includes neither a private right of action nor a breach notification provision.[231] The statute is directed towards internet service providers (ISPs)[232] and generally only prohibits the types of data ISPs can collect and use;[233] however, ISPs are required to implement protective measures for that data to prevent unauthorized access.[234] Though the least protective of consumers overall, the Maine legislation is a useful indicator that states are not only trending toward arming potential data breach plaintiffs, but actually enacting laws to put the swords in their hands.

c. Selected Proposed Legislation in Other States

Many states are currently considering legislation that would protect individuals' data to some degree.[235] In New York and South Carolina, laws would require notification of a data breach to affected consumers.[236] In Illinois, Maryland, New Hampshire, New York, and South Carolina, proposed legislation provides a private right of action to the individuals affected by a data breach.[237] Illinois, Iowa, and Minnesota also have pending laws that would require routine risk assessments, but obviously this would be a much narrower protection than breach notifications or rights of action.[238] Finally, a number of states have moved proposed legislation to a task force to study this area in greater detail, effectively preserving the potential for widespread data protection.[239]

---

[229] *See id.* § 603A.220.

[230] *See* ME. REV. STAT. ANN. tit. 35-A, § 9301 (West 2020).

[231] *See id.*

[232] *Id.* § 9301(1)(D).

[233] *See generally id.* § 9301.

[234] *See id.* § 9301(5).

[235] *See* Rippy, *supra* note 220.

[236] *See* S.B. 5642, State Assemb., 2019–20 Sess. (N.Y. 2019); H.B. 4812, 123d Gen. Assemb., 2019–2020 Sess. (S.C. 2019) (referring only to collected biometric data).

[237] *See* H.B. 5603, 101st Gen. Assemb., 2019 & 2020 Reg. Sess. (Ill. 2020); S.B. 2330, 101st Gen. Assemb., 2019 & 2020 Reg. Sess. (Ill. 2020); H.B. 1656, 2020 Gen. Assemb., Reg. Sess. (Md. 2020); H.B. 1680, Gen. Court, 2020 Sess. (N.H. 2020); N.Y. S.B. 5642; S.C. H.B. 4812.

[238] *See* Ill. S.B. 2330; S.B. 2263, 101st Gen. Assemb., 2019 & 2020 Reg. Sess. (Ill. 2019); S. File 2351, 88th Gen. Assemb., Reg. Sess. (Iowa 2020) (as amended by S-5084 on Mar. 11, 2020); H. File 3936, 91st Leg., Reg. Sess. (Minn. 2020).

[239] Connecticut, Hawaii, Louisiana, Massachusetts, North Dakota, and Texas all fall into this category. *See* Rippy, *supra* note 220.

B. The Court Must Act Despite Congressional Inaction

It is ultimately within the courts' purview to act as an engine of social change when legislatures fail to perform the same function.[240] And the importance of heightened security for at least certain tiers of personal data cannot be overstated. Some data, like Social Security numbers or medical records, cannot be cancelled (like the cancelled credit card the Second Circuit relied on to deny standing in *Whalen v. Michaels Stores, Inc.*[241]); therefore, risk of identity theft when this type of data is stolen may continue on forever.[242] Those entities entrusted with sensitive personal data must be held to rigorous standards to encourage the highest possible safety standards and prevent the theft of data which could severely, and perpetually, burden victims of data breaches.

Illustrative of why the Court must act if Congress declines to legislate is the Third Circuit's holding in *Horizon Healthcare*.[243] After laptops containing "unencrypted" sensitive data, including in some cases health history and Social Security numbers, were stolen from defendant's premises, affected plaintiffs filed suit.[244] The Third Circuit granted standing to the plaintiffs under the Fair Credit Reporting Act (FCRA).[245] The court held that rather than clarifying the injury in fact requirement, *Spokeo* emphasized Congress's power to create standing, which guided the *Horizon Healthcare* court's rationale.[246] The court noted that without passage of the FCRA, the instant plaintiffs would otherwise have no opportunity to redress their injuries.[247] To be sure, the court did not foreclose the idea that a breach by itself can tend to

---

[240] *See* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 314 ("Historically, courts have occasionally participated in social changes by modernizing the law when legislatures have been slow to respond to emerging trends."); *see also* Heather K. Gerken, *The Supreme Court Is a Partner in Transformation, Not the Sole Agent*, N.Y. TIMES (July 7, 2015, 2:20 AM), https://www.nytimes.com/roomfordebate/2015/07/06/is-the-supreme-court-too-powerful/the-supreme-court-is-a-partner-in-transformation-not-the-sole-agent [https://perma.cc/AGJ4-RAN2] (noting that with respect to the social groundswell leading to United States v. Windsor, 570 U.S. 744 (2013), "the courts haven't been in the lead in effecting change, but they have been an integral part of the process of change").

[241] 689 F. App'x 89, 90–91 (2d Cir. 2017).

[242] Unfortunately, "forever" is not an exaggeration. *See* Kirchheimer, *supra* note 158.

[243] *See In re* Horizon Healthcare Servs. Inc. Data Breach Litigation, 846 F.3d 625 (3d Cir. 2017).

[244] *Id.* at 630–31.

[245] *See id.* at 634–35.

[246] *See id.* at 638–41.

[247] *See id.* at 638–40*; see also id.* at 643 (Shwartz, J., concurring in the judgment) (writing separately to make clear that the plaintiffs' alternative theory of liability through a risk of future harm would have been unavailing had the court found it necessary to rule beyond the baseline FCRA unauthorized disclosure theory).

show an injury in fact,[248] but the court's analysis depended upon an existent federal statute.[249]

Horizon Healthcare perfectly encapsulates the dangerous confusion the Court is well-positioned to quell. Without a congressional framework for data breach litigation, litigants are left with piecemeal federal opportunities—by statute or court—to remedy likely forthcoming losses from stolen data, begetting the circuit split, and with some, potentially many, victims falling through the cracks in the current patchwork system.

CONCLUSION

The consequences of data breaches are too steep for the ultimate victims, data breach litigation plaintiffs, to suffer without proper opportunity for recourse. Because the current landscape of standing in data breach litigation continues to vacillate, although recently trending towards plaintiff-victims, the Court must revisit its approach to standing for data breach cases, regardless of whether Congress presents the Court an opportunity to do so through federal overhaul legislation.

The current circuit split over Article III standing in data breach litigation carries the potential for resolution without upheaval. This Note advances three potential solutions, any one of which would significantly ease the encumbrances on data breach victims. But the "tiered sensitivity" approach provides substantial incentive for each interested faction to accept the change without controversy: a heavy enough sword for plaintiffs to recoup most losses, fairness for defendants to avoid permanent liability in all cases, and an adequate shield for courts to maintain jurisdiction over truly justiciable cases. Because the Court's own jurisprudence over the past half-century supports revisiting and reshaping the standing doctrine morass, the Court should follow the example of legislatures at home and abroad to step in and effect a necessary social protection for data breach plaintiffs in pursuit of lawful recovery.

---

[248] *But see id.* at 643–44. Similar to the Fourth Circuit in Beck v. McDonald, 848 F.3d 262, 274–75 (4th Cir. 2017), Judge Shwartz would require a thief to know what the laptop contained and have targeted it specifically to exploit that information. Neither Judge Shwartz's concurrence nor the majority opinion discuss the proper result in a classic breach scenario (i.e., hackers penetrating a digital firewall). *See generally Horizon Healthcare*, 846 F.3d at 625–44.

[249] *Id.* at 639.