DATA BREACHES, IDENTITY THEFT, AND ARTICLE III STANDING: WILL THE SUPREME COURT RESOLVE THE SPLIT IN THE CIRCUITS?

*Bradford C. Mank**

* James Helmer, Jr. Professor of Law and Associate Dean for Academic Affairs, University of Cincinnati College of Law, P.O. Box 210040, University of Cincinnati, Cincinnati, Ohio 45221-0040, Telephone 513-556-0094, Fax 513-556-1236, e-mail: brad.mank@uc.edu. All errors or omissions are my responsibility.

This Article is one of a series of explorations of modern standing doctrines. The other pieces are: (1) Bradford Mank, *Should States Have Greater Standing Rights than Ordinary Citizens?:* Massachusetts v. EPA*'s New Standing Test for States*, 49 Wm. & Mary L. Rev. 1701 (2008) [hereinafter Mank, *State Standing*]; (2) Bradford C. Mank, *Standing and Future Generations: Does* Massachusetts v. EPA *Open Standing for Generations to Come?*, 34 Colum. J. Envtl. L. 1 (2009) [hereinafter Mank, *Standing and Future Generations*]; (3) Bradford Mank, *Standing and Statistical Persons: A Risk-Based Approach to Standing*, 36 Ecology L.Q. 665 (2009); (4) Bradford Mank, Summers v. Earth Island Institute *Rejects Probabilistic Standing, but a "Realistic Threat" of Harm Is a Better Standing Test*, 40 Envtl. L. 89 (2010); (5) Bradford Mank, *Revisiting the* Lyons *Den:* Summers v. Earth Island Institute*'s Misuse of* Lyons*'s "Realistic Threat" of Harm Standing Test*, 42 Ariz. St. L.J 837 (2010); (6) Bradford C. Mank, Summers v. Earth Island Institute*: Its Implications for Future Standing Decisions*, 40 Envtl. L. Rep. 10958 (2010); (7) Bradford Mank, *Standing in* Monsanto Co. v. Geertson Seed Farms*: Using Economic Injury as a Basis for Standing When Environmental Harm Is Difficult to Prove*, 115 Penn St. L. Rev. 307 (2010); (8) Bradford C. Mank, *Informational Standing After* Summers, 39 B.C. Envtl. Aff. L. Rev. 1 (2012); (9) Bradford C. Mank, *Reading the Standing Tea Leaves in* American Electric Power Co. v. Connecticut, 46 U. Rich. L. Rev. 543 (2012); (10) Bradford C. Mank, *Judge Posner's "Practical" Theory of Standing: Closer to Justice Breyer's Approach to Standing than to Justice Scalia's*, 50 Houston L. Rev. 71 (2012); (11) Bradford C. Mank, *Standing for Private Parties in Global Warming Cases: Traceable Standing Causation Does Not Require Proximate Causation*, 2012 Mich. St. L. Rev. 869 (2012); (12) Bradford C. Mank, *Is Prudential Standing Jurisdictional?*, 64 Case W. L. Rev. 413 (2013); (13) Bradford C. Mank, Clapper v. Amnesty International*: Two or Three Competing Philosophies of Standing Law?*, 81 Tenn. L. Rev. 211 (2014) [hereinafter Mank, *Two or Three*]; (14) Bradford C. Mank, *No Article III Standing for Private Plaintiffs Challenging State Greenhouse Gas Regulations: The Ninth Circuit's Decision in* Washington Environmental Council v. Bellon, 63 Am. U. L. Rev. 1525 (2014); (15) Bradford C. Mank, *Does* United States v. Windsor *(the DOMA Case) Open the Door to Congressional Standing Rights?*, 76 U. Pitt. L. Rev. 1 (2014).

ABSTRACT

In data breach cases, the plaintiff typically alleges that the defendant used inadequate computer security to protect the plaintiff's personal data. In most, but not all cases, the plaintiff cannot prove that a hacker or thief has actually used or sold the data to the plaintiff's detriment. In most cases, a plaintiff alleges that the defendant's failure to protect his personal data has caused him damages by increasing his risk of suffering actual identity theft in the future and therefore imposed costs on the plaintiff when he reasonably takes measures to prevent future unauthorized third-party data access by purchasing credit monitoring services.

In data breach cases, the lower federal courts have split on the question of whether the plaintiffs meet Article III standing requirements for injury and causation. In its 2013 decision Clapper v. Amnesty International USA, the Supreme Court, in a case involving alleged electronic surveillance by the U.S. government's National Security Agency, declared that a plaintiff alleging that it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are "certainly impending." Since the Clapper decision, a majority of the lower federal courts addressing "lost data" or potential identity theft cases in which there is no proof of actual misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data. But a significant minority of lower court decisions have disagreed that the Clapper decision requires denial of standing in data breach cases in which there is no proof of present harm, because a footnote in Clapper acknowledged that the Court had sometimes used a less strict "substantial risk" test when plaintiffs alleged that a defendant's actions increase their risk of future harm.

Demonstrating its concern for digital privacy, the Court in Riley v. California recently required police to obtain a Fourth Amendment warrant before examining the digital data on the cell phones of arrested suspects. It would be easy for courts to distinguish the government's seizure of digital data from arrestees in Riley from a third party's hacking of data from a retailer or employer. The Riley decision involves Fourth Amendment warrant issues that are not relevant to private data breach cases. Yet in both cell phone seizure cases and data breach cases, there is the common concern that vast amounts of personal data are often at stake. The new privacy concerns in a digital age should lead the Supreme Court to take a broader view of standing in data breach cases. It is also possible that the Court will follow the Seventh Circuit's Remijas *decision to distinguish between cases where there is only a possible risk of theft from those where actual harm has occurred to some plaintiffs.*

INTRODUCTION

Because Article III of the Constitution limits the authority of federal judges to deciding "Cases" and "Controversies,"[1] the U.S. Supreme Court has interpreted Article III to impose mandatory standing requirements that require each plaintiff in federal court to demonstrate that he has suffered a concrete injury that is fairly traceable to the actions of the defendant and redressable by a favorable judgment of a federal court.[2] The injury and traceable causation prongs of the Article III standing test have raised problems for plaintiffs in "lost data," "data breach," or potential "identity theft" cases in which plaintiffs allege damages when computer hackers or thieves of physical property such as laptops or hard drives breach a defendant's computer system or network that contains the plaintiff's personal

1 U.S. CONST. art. III, § 2; *see also infra* Part I.

2 *See infra* Part I.

information such as birth dates or Social Security numbers.[3] Data breach cases can involve tens of millions of Americans, as in the Target retail breach, which led to sixty-eight class action lawsuits[4] in twenty-one states and the District of Columbia in less than one month,[5] and, therefore these cases raise important policy concerns.[6]

In data breach cases, the plaintiff typically alleges that the defendant used inadequate computer security to protect the plaintiff's personal data from being accessed by third party hackers or thieves.[7] In most, but not all cases, the plaintiff cannot prove that a hacker or thief has actually used or sold the data to the plaintiff's detriment.[8] In most cases, a plaintiff alleges that the defendant's failure to protect his personal data has caused him damages by increasing his risk of suffering actual identity theft in the future and therefore imposed costs on the plaintiff when he reasonably takes measures

3 *See infra* Part III. *See generally* Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 CARDOZO L. REV. DE NOVO 119, 120–21, 127–28 (arguing that courts should reject third-party doctrine that citizens surrender any privacy rights voluntarily conveyed to a third party, and allow standing in data breach cases); Lexi Rubow, Note, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1040–42 (2014) (advocating broader standing in data breach cases).

4 *See generally* FED. R. CIV. P. 23 (setting forth rules for certifying class actions in federal courts); Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 414–19 (2014) (discussing issues involving data breach plaintiffs seeking class certification pursuant to Federal Rule of Civil Procedure 23). Named plaintiffs in a class action must prove Article III standing, but lower courts have divided over whether absent class members also have to demonstrate standing. *See generally* Theane Evangelis & Bradley J. Hamburger, *Article III Standing and Absent Class Members*, 64 EMORY L.J. 383 (2014). A full discussion of the standing of class members is beyond the scope of this Article.

5 Joel Schectman, *Target Faces Nearly 70 Lawsuits over Breach*, WALL ST. J. (Jan. 15, 2014), http://blogs.wsj.com/riskandcompliance/2014/01/15/target-faces-nearly-70-lawsuits-over-breach/.

6 *See* John L. Jacobus & Benjamin B. Watson, Clapper v. Amnesty International *and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 1, 1 (2014) ("While Target originally estimated that the security breach affected 40 million of its customers, a subsequent investigation revealed that anywhere from 70 to 110 million people—almost one in three Americans—may have had their sensitive payment information stolen."); Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1173–74 (2014) (discussing data breach cases involving millions of customers each at Target, Home Depot, and JP Morgan Chase).

7 *See* Cease, *supra* note 4, at 399 (discussing cases "in which the plaintiffs' information has been accessed but that information has not been used to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiffs. However, these plaintiffs typically claim that they have been harmed in other ways: incurring costs for credit-monitoring services, paying the costs of cancelling and receiving new bank cards, suffering loss of reward points from cancelled cards, and enduring general anxiety that their information will be used in the future to make unauthorized purchases." (footnote omitted)); *see also infra* Part III.

8 *See infra* Part III; *see also* Cease, *supra* note 4, at 399–404.

to prevent future unauthorized third-party data access by purchasing credit monitoring services.[9] However, if a plaintiff's credit cards or bank accounts have actually been misused by thieves because of a data breach, then there is a much stronger argument that the plaintiff has demonstrated standing injury and causation.[10]

Currently, there is no comprehensive federal statute addressing data breach issues so plaintiffs have invoked a variety of state and federal laws to sue defendant companies that have failed to protect the plaintiffs' data.[11] For example, some of the cases are brought under state common law negligence or breach of contract theories, and others pursuant to federal statutes such as the Fair Credit Reporting Act (FCRA).[12] A related issue arises where a defendant has allegedly falsely reported information about a plaintiff to third parties in violation of various federal statutes, but it is difficult to measure the actual harm to the plaintiff.[13]

---

9 *See* Cease, *supra* note 4, at 399–404; *infra* Part III.

10 *See* Resnick v. AvMed, Inc., 693 F.3d 1317, 1322–23 (11th Cir. 2012) (holding that a plaintiff's allegation that a third party opened bank accounts in the plaintiff's name and caused financial losses is a sufficient injury in fact for Article III standing); Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008) (concluding that a plaintiff's "actual financial injuries are sufficient to meet the injury-in-fact requirement" for Article III standing); Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 665 (E.D. Pa. 2015) (holding the plaintiff had standing where his credit cards or bank accounts had actually been misused by thieves because of a data breach for which defendant had responsibility); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (same); Cease, *supra* note 4, at 398–99 (discussing Sixth and Eleventh Circuit decisions holding that plaintiffs have Article III standing if a data breach results in financial charges against a plaintiff); Peters, *supra* note 6, at 1188 (discussing *Resnick*). Courts have divided over standing when a defendant has reimbursed all direct costs of a financial misuse of stolen information, but plaintiffs allege that they have suffered serious indirect or incidental costs from significant time spent correcting fraudulent charges, or where they could not access their credit or bank accounts for a period of time as a result of a breach. *Compare Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688, 692–97 (7th Cir. 2015) (concluding 9200 plaintiffs who were later reimbursed for fraudulent charges had alleged an adequate injury in fact for standing where they alleged that they had "suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers [were] changed, and to pursue relief for unauthorized charges"), *with* Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1284–85 (N.D. Ala. 2014) (concluding the plaintiff must incur actual unreimbursed damages to have either standing or a ripe claim). *See also* Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, 84 U.S.L.W. (BNA) 488 (Oct. 13, 2015) (discussing *Remijas* and citing *Burton*).

11 *See* Peters, *supra* note 6, at 1177–83 (discussing several federal and state statutes relevant to victims of data breaches).

12 *See* Cease, *supra* note 4, at 405–13 (discussing state common law and statutory claims in data breach cases); Peters, *supra* note 6, at 1177–87, 1194 (observing that only fourteen states provide a private cause of action for data breaches, that there is no comprehensive federal statute giving a private right of action for data breaches, and, therefore, data breach plaintiffs in most states must bring either common law actions or more indirect state or federal statutory claims); *infra* Part III.

13 *See infra* Part III.

In data breach cases, and also in false reporting cases, the lower federal courts have split on the question of standing.[14] In its 2013 decision *Clapper v. Amnesty International USA*,[15] the Supreme Court, in a case involving alleged electronic surveillance by the U.S. government's National Security Agency, declared that a plaintiff alleging that it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are "certainly impending."[16] Since the *Clapper* decision, a majority of the lower federal courts addressing "lost data" or potential identity theft cases in which there is no proof of actual misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data.[17] But a significant minority of lower court decisions have disagreed that the *Clapper* decision requires denial of standing in all data breach cases, because a footnote in *Clapper* acknowledged that the Court had sometimes used a less strict "substantial risk" test when plaintiffs alleged that a defendant's actions increase their risk of future harm.[18] Furthermore, the Seventh Circuit in its 2015 decision *Remijas v. Neiman Marcus Group, LLC*, distinguished *Clapper* because a significant number of the plaintiffs had suffered actual fraud or other harms, on the grounds that in such cases other plaintiffs are at increased risk compared to cases where no one has suffered an actual theft of property.[19]

In light of the continuing split in the circuits regarding Article III standing in data breach and fraudulent reporting cases, the Supreme Court will eventually have to address this important question.[20] Predicting how the Court will resolve the issue is difficult because the Court's standing precedents could plausibly support either position.[21] It is possible that the Court's decision will depend on how personally vulnerable some of the Justices feel to the threat of identity theft.[22] Alternatively, the Court may follow the Seventh Circuit's *Remijas* decision to distinguish cases where there is only a possi-

14 *See infra* Part III.

15 133 S. Ct. 1138 (2013).

16 *Id.* at 1143 (internal quotation marks omitted); *see also infra* Part II.

17 *See infra* Part III.

18 *Clapper*, 133 S. Ct. at 1150 n.5; *see also infra* Parts II, III.

19 *See Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688, 692–94 (7th Cir. 2015); John Biglow, Note, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 955–57, 967–69, 972–73, 975 (2016) (discussing and praising the Seventh Circuit's decision in *Remijas*); Clara Kim, Note, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 573–77 (same); Rajesh De et al., *The Evolution of Data Breach Litigation in the United States: What's Happening and What's Ahead*, 84 U.S.L.W. (BNA) 710 (Nov. 24, 2015) (arguing that some courts have distinguished *Clapper* in data breach suits where some plaintiffs have suffered actual injuries); *infra* Section III.D.

20 *See infra* Part III, Conclusion.

21 *See infra* Part III, Conclusion.

22 *See infra* Conclusion.

ble risk of theft from those where actual harm has occurred to some plaintiffs.[23]

Demonstrating its concern for digital privacy, the Court recently required police to obtain a Fourth Amendment warrant before examining the digital data on the cell phones of arrested suspects in *Riley v. California*.[24] It would be easy for courts to distinguish the government's seizure of digital data from arrestees in *Riley* from a third party's hacking of data from a retailer or employer.[25] The *Riley* decision involves Fourth Amendment warrant issues that are not relevant to private data breach cases against companies that failed to protect data.[26] However, in both cell phone seizure cases and data breach cases, there is a similar policy concern that huge amounts of personal data are often at risk.[27] The *Riley* decision's recognition of new privacy concerns in a digital era should lead the Supreme Court to take a broader view of standing in data breach cases.[28]

Part I explains the basic principles of constitutional Article III standing.[29] Part II discusses how the recent *Clapper* and *Susan B. Anthony List v. Driehaus*[30] decisions arguably affect when plaintiffs have Article III standing based on future injuries.[31] Part III examines the split in the circuits regarding Article III standing in data breach and fraudulent reporting cases and the impact of the *Clapper* and *Susan B. Anthony* decisions on how lower federal courts decide standing.[32] The Conclusion discusses whether the Court's recent Fourth Amendment decision protecting the privacy of cell phone data might have implications in standing cases involving data breaches.[33]

I. Introduction to Constitutional Article III Standing

While the Constitution does not explicitly mandate that each and every plaintiff demonstrate "standing" to file suit in federal courts, the Supreme Court has inferred from Article III's limitation of judicial decisions to "Cases" and "Controversies" that federal courts must impose standing requirements to establish that a plaintiff has a genuine interest and a stake in the outcome

23 *See Remijas*, 794 F.3d at 692–97; Biglow, *supra* note 19, at 972–73, 975 (arguing courts should follow the Seventh Circuit's decision in *Remijas*, which found Article III standing where some persons had already been harmed by a data breach and remaining plaintiffs were therefore at a significantly increased risk of harm); *infra* Section III.D.

24 134 S. Ct. 2473, 2493 (2014); *see infra* Conclusion.

25 *See infra* Conclusion.

26 *See infra* Conclusion.

27 *See infra* Conclusion.

28 *See infra* Conclusion.

29 *See infra* Part I. The discussion of standing in Part I relies upon my earlier standing articles. *See supra* note *.

30 134 S. Ct. 2334 (2014).

31 *See infra* Part II.

32 *See infra* Part III.

33 *See infra* Conclusion.

of a case.[34] For a federal court to have jurisdiction over a claim, at least one plaintiff must prove it has standing for each form of relief sought.[35] Federal courts must dismiss a case if no plaintiff meets constitutional Article III standing requirements.[36]

Standing requirements are based upon fundamental constitutional principles. Standing doctrine prohibits unconstitutional advisory opinions.[37] Furthermore, standing requirements are congruent with separation of powers principles defining the division of powers between the judiciary and political branches of government so that the "Federal Judiciary respects 'the proper—and properly limited—role of the courts in a democratic society.'"[38] Various members of the Supreme Court have disagreed, however,

---

34 The constitutional standing requirements are derived from Article III, Section 2, which provides:

> The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public Ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—[between a State and Citizens of another State;—] between Citizens of different States,—between Citizens of the same State claiming Lands under Grants of different States, [and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.]

U.S. CONST. art. III, § 2 (footnote omitted); *see also* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 340–41 (2006) (explaining why the Supreme Court infers that Article III's case and controversy requirement necessitates standing limitations and clarifying that "[i]f a dispute is not a proper case or controversy, the courts have no business deciding it"); Stark v. Wickard, 321 U.S. 288, 310 (1944) (stating that Article III grants courts the power to "adjudicate cases and controversies as to claims of infringement of individual rights whether by unlawful action of private persons or by the exertion of unauthorized administrative power"). *See generally* Michael E. Solimine, *Congress, Separation of Powers, and Standing*, 59 CASE W. RES. L. REV. 1023, 1036–38 (2009) (discussing a scholarly debate on whether the framers intended the Constitution to require standing to sue).

35 *See DaimlerChrysler*, 547 U.S. at 352 (confirming that "a plaintiff must demonstrate standing separately for each form of relief sought" (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 185 (2000) (internal quotation marks omitted))); Mank, *State Standing*, *supra* note *, at 1710.

36 *See DaimlerChrysler*, 547 U.S. at 340–41 (emphasizing the importance of the case or controversy requirement); *Friends of the Earth*, 528 U.S. at 180 (adding that courts have an affirmative duty at the outset of the litigation to ensure that litigants satisfy all Article III standing requirements).

37 *See* Chafin v. Chafin, 133 S. Ct. 1017, 1023 (2013) ("Article III of the Constitution restricts the power of federal courts to 'Cases' and 'Controversies.' Accordingly, '[t]o invoke the jurisdiction of a federal court, a litigant must have suffered, or be threatened with, an actual injury traceable to the defendant and likely to be redressed by a favorable judicial decision.' Federal courts may not 'decide questions that cannot affect the rights of litigants in the case before them' or give 'opinion[s] advising what the law would be upon a hypothetical state of facts.'" (alterations in original) (citations omitted) (quoting Lewis v. Cont'l Bank Corp., 494 U.S. 472, 477 (1990))).

38 *DaimlerChrysler*, 547 U.S. at 341 (internal quotation marks omitted) (quoting Allen v. Wright, 468 U.S. 737, 750 (1984), *partially abrogated by* Lexmark Int'l, Inc. v. Static Con-

regarding the degree to which separation of powers principles limit Congress's authority to authorize standing to sue in federal courts for private-citizen suits challenging executive branch under- or non-enforcement of congressional requirements that are arguably mandated by statute.[39]

The Supreme Court has established a three-part test for constitutional Article III standing that requires a plaintiff to show that: (1) she has "suffered an injury in fact," which is (a) "concrete and particularized"[40] and (b) "actual or imminent, not 'conjectural' or 'hypothetical'";[41] (2) "there [is] a causal connection between the injury and the conduct complained of—the injury has to be 'fairly . . . trace[able][42] to the challenged action of the defendant, and not . . . th[e] result[ ] [of] the independent action of some third party not before the court'";[43] and (3) "it [is] 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[44] The

---

trol Components, Inc., 134 S. Ct. 1377 (2014)); *see also* Mank, *Standing and Future Generations*, *supra* note *, at 26.

39 *Compare* Lujan v. Defenders of Wildlife, 504 U.S. 555, 573–78 (1992) (concluding that Articles II and III of the Constitution limit Congress's authority to authorize citizen suits by any person lacking a concrete injury, and citing several recent Supreme Court decisions for support), *with id.* at 580 (Kennedy, J., concurring in part and concurring in the judgment) ("Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before"), *and id.* at 602 (Blackmun, J., dissenting) (arguing that the "principal effect" of the majority's approach to standing was "to transfer power into the hands of the Executive at the expense—not of the courts—but of Congress, from which that power originates and emanates"). *See generally* Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459, 496 (2008) (suggesting the "disagreement" is "[u]nsurprising[ ]" and arguing that courts should not use standing doctrine as "a backdoor way to limit Congress's legislative power").

40 *Lujan*, 504 U.S. at 560 (internal quotation marks omitted) (citing *Allen*, 468 U.S. at 756).

41 *Id.* (internal quotation marks omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

42 The *Lexmark* decision explained the distinction between the standing requirement of fairly traceable causation and the ultimate question of proving proximate causation on the merits as follows:

> Proximate causation is not a requirement of Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct. Like the zone-of-interests test, it is an element of the cause of action under the statute, and so is subject to the rule that "the absence of a valid (as opposed to arguable) cause of action does not implicate subject-matter jurisdiction." But like any other element of a cause of action, it must be adequately alleged at the pleading stage in order for the case to proceed. If a plaintiff's allegations, taken as true, are insufficient to establish proximate causation, then the complaint must be dismissed; if they are sufficient, then the plaintiff is entitled to an opportunity to prove them.

Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1391 n.6 (2014) (citations omitted) (quoting Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 89 (1998)) (citing Ashcroft v. Iqbal, 556 U.S. 662, 678–79 (2009)).

43 *Lujan*, 504 U.S. at 560 (second, third, fourth, fifth, and seventh alterations in original) (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41–42 (1976)).

44 *Id.* at 561 (quoting *Simon*, 426 U.S. at 38, 43).

plaintiff bears the burden of proving all three elements of constitutional Article III standing.[45]

In several cases, but not every decision, the Court has established a standing principle that a party "generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties."[46] The Court has explained its third-party standing doctrine as assuming that "the party with the right has the appropriate incentive to challenge (or not challenge) governmental action and to do so with the necessary zeal and appropriate presentation," but that third parties are more likely to raise "abstract questions of wide public significance" that are better addressed by "other governmental institutions" than the federal courts.[47] The Court has allowed exceptions to the general limitation on third-party standing in some constitutional areas involving fundamental rights.[48] However, the Court has restricted those exceptions

> by requiring that a party seeking third-party standing make two additional showings. First, we have asked whether the party asserting the right has a "close" relationship with the person who possesses the right. Second, we have considered whether there is a "hindrance" to the possessor's ability to protect his own interests.[49]

In cases involving First Amendment and other critical constitutional rights, the Court has been more willing to acknowledge third-party suits, but in non-constitutional areas of law, the Court has been much less willing to do so.[50]

The Court's limitation of third-party suits to important constitutional questions helps to explain a somewhat related principle that parties that voluntarily transfer information to another party generally cannot sue for invasion of privacy if the receiving party knowingly or inadvertently conveys that

---

45 *See* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 342 (2006) (stating that parties asserting federal jurisdiction must "carry the burden of establishing their standing under Article III"); *Lujan*, 504 U.S. at 561 ("The party invoking federal jurisdiction bears the burden of establishing these elements."); Bradford C. Mank, *Prudential Standing Doctrine Abolished or Waiting for a Comeback?:* Lexmark International, Inc. v. Static Control Components, Inc., 18 U. PA. J. CONST. L. 213, 220 (2015) ("The plaintiff bears the burden of proof for all three prongs of constitutional Article III standing.").

46 Kowalski v. Tesmer, 543 U.S. 125, 129 (2004) (internal quotation marks omitted) (quoting Warth v. Seldin, 422 U.S. 490, 499 (1975), *partially abrogated by Lexmark*, 134 S. Ct. 1377 (2014)); *see also* Mank, *supra* note 45, at 258.

47 *Kowalski*, 543 U.S. at 129 (internal quotation marks omitted) (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975), *partially abrogated by Lexmark*, 134 S. Ct. 1377); *see also* Mank, *supra* note 45, at 258.

48 *Kowalski*, 543 U.S. at 129–30; Brandon L. Garrett, *The Constitutional Standing of Corporations*, 163 U. PA. L. REV. 95, 147–49 (2014); Mank, *supra* note 45, at 258. *See generally* Brian Charles Lea, *The Merits of Third Party Standing*, 24 WM. & MARY BILL RTS. J. 277, 287–302 (2015) (discussing history of third-party standing doctrine).

49 *Kowalski*, 543 U.S. at 130 (citations omitted) (quoting Powers v. Ohio, 499 U.S. 400, 411 (1991)); Garrett, *supra* note 48, at 147–49; Mank, *supra* note 45, at 258.

50 Mank, *supra* note 45, at 258–61 (citing several cases); *see* Lea, *supra* note 48, at 296–302 (same).

information to third parties, including hackers.[51] In *Katz v. United States*, the Supreme Court held that the Fourth Amendment's protection against unreasonable government searches applies only if a person has a reasonable expectation of privacy in the information seized by the government.[52] The *Katz* decision's "reasonable expectation of privacy" principle has been applied outside its original Fourth Amendment context to deny privacy rights to plaintiffs who voluntarily convey information to another party that is accessed by a third party.[53] If a plaintiff lacks a privacy expectation in unlawfully accessed data, arguably there is no injury from the release of the information itself in the absence of actual financial harm, or from possible future injuries from misuse of that information.[54] However, the Conclusion will argue that traditional limitations on privacy doctrines should be revised in an online era where personal data is readily accessible to unwanted third parties, including hackers or the government.[55]

II. *CLAPPER*, "SUBSTANTIAL RISK," AND *SUSAN B. ANTHONY LIST V. DRIEHAUS*

The Supreme Court has used arguably conflicting tests for when a plaintiff's allegations about potential future injuries are sufficiently imminent to constitute an injury for Article III standing.[56] In its 2013 decision *Clapper v. Amnesty International USA*,[57] the Court, in a sharply divided 5-4 decision, with a majority opinion written by Justice Alito, announced that a plaintiff alleging it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are "certainly impending,"[58] which is a very strict standard of proof.[59] The decision was arguably vague or ambiguous about whether the strict, "certainly impending"[60] test was limited to cases in which the government is involved in the use of espionage, as in *Clapper*, to protect the nation's national security or whether that test is more generally applicable in other factual scenarios.[61] Furthermore, the *Clapper* decision

51 Lamparello, *supra* note 3, at 120–21.

52 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Lamparello, *supra* note 3, at 121.

53 *See* Lamparello, *supra* note 3, at 121.

54 *Id.* at 126–28.

55 *See infra* Conclusion; *see also* Lamparello, *supra* note 3, at 120–21, 127–29.

56 *See* Marty Lederman, *Commentary:* Susan B. Anthony List, Clapper Footnote 5, and the State of Article III Standing Doctrine, SCOTUSBLOG (June 17, 2014, 4:34 PM), http://www.scotusblog.com/2014/06/commentary-susan-b-anthony-list-clapper-footnote-5-and-the-state-of-article-iii-standing-doctrine/ (discussing the conflict on the Court between the "certainly impending" test for future injuries and the "substantial risk" test); *see also* Mank, *Two or Three*, *supra* note *, at 222–40.

57 133 S. Ct. 1138 (2013).

58 *Id.* at 1143.

59 *See* Jacobus & Watson, *supra* note 6, at 10–15 (discussing *Clapper*); Mank, *Two or Three*, *supra* note *, at 222–40 (same); Lederman, *supra* note 56 (same).

60 *Clapper*, 133 S. Ct. at 1143.

61 As previously stated:

> The *Clapper* decision sent mixed signals about whether its approach to standing was generally applicable to all cases or whether it was more limited to stand-

arguably involved separation of powers and political-question-doctrine issues not present in data breach cases involving private parties.[62] However, in a footnote, the *Clapper* majority opinion acknowledged in response to Justice Breyer's dissenting opinion that the Court had sometimes used a less strict "substantial risk" test.[63] Since the *Clapper* decision, some lower courts have applied or discussed using the alternative, "substantial risk" standard in *Clapper*.[64]

In 2014, the Court in *Susan B. Anthony List v. Driehaus*,[65] a unanimous decision written by Justice Thomas, suggested that a plaintiff, in some circumstances, need only establish a substantial risk of future harm to demonstrate Article III standing. An Ohio statute "makes it a crime for any person to '[m]ake a false statement concerning the voting record of a candidate or public official.'"[66] During the 2010 election cycle, Susan B. Anthony List (SBA), a "pro-life advocacy organization," accused then-Congressman Steve Driehaus, who was running for re-election to Congress, of supporting a healthcare bill that purportedly provided taxpayer-funded abortion procedures.[67] In response, Congressman Driehaus filed a complaint with the Ohio Elections Commission alleging that SBA's claims violated the false-statement statute.[68] In October 2010, responding to his complaint, the Commission in

---

> ing in intelligence-gathering and foreign affairs cases. As the majority observed, "we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." The Court then cited three prior decisions that had denied standing to plaintiffs in cases involving intelligence or military affairs. The question that the *Clapper* Court never fully answered is whether its narrow interpretations of both the "certainly impending" injury requirement and the "fairly traceable" causation requirement are only applicable to intelligence and foreign affairs cases or more broadly applicable to standing questions in a wide variety of contexts. The text of the majority opinion suggests that the "certainly impending" test is broadly applicable, but footnote 5 raises serious questions about the test.

Mank, *Two or Three*, *supra* note *, at 225–26 (footnotes omitted) (quoting *Clapper*, 133 S. Ct. at 1147).

62 *See Clapper*, 133 S. Ct. at 1146; Jacobus & Watson, *supra* note 6, at 64–65.

63 *Clapper*, 133 S. Ct. at 1150 n.5.

64 *See, e.g.*, Hedges v. Obama, 724 F.3d 170, 196–97 (2d Cir. 2013) (discussing and applying the "substantial risk" test from *Clapper* as a means for pre-enforcement review of possible criminal charges), *cert. denied*, 134 S. Ct. 1936 (2014) (mem.); Organic Seed Growers and Trade Ass'n v. Monsanto Co., 718 F.3d 1350, 1355–56 (Fed. Cir. 2013) (concluding the plaintiff met the "substantial risk" test in *Clapper*), *cert. denied*, 134 S. Ct. 901 (2014) (mem.); Nat. Res. Def. Council v. FDA, 710 F.3d 71, 82–83 (2d Cir. 2013) (distinguishing *Clapper* on the grounds that health risks from the chemical triclosan were not "highly speculative"); Mank, *Two or Three*, *supra* note *, at 264–74 (discussing cases).

65 134 S. Ct. 2334, 2341 (2014).

66 *Id.* at 2338–39 (alteration in original) (discussing and quoting the Ohio false statement statute, OHIO REV. CODE ANN. § 3517.21(B)(9) (West 2016), and related statutes).

67 *Id.* at 2339 (internal quotation marks omitted) (quoting Susan B. Anthony List v. Driehaus, 525 Fed. App'x 415, 416 (6th Cir. 2013)).

68 *Id.*

a preliminary decision "voted 2 to 1 to find probable cause that a violation had been committed" by SBA.[69] SBA then unsuccessfully sought injunctive relief from a federal district court and then the Sixth Circuit to block the Commission from holding a final hearing on the merits of the case.[70] SBA and Driehaus agreed to postpone the hearing until after the November 2010 election.[71] After he lost the congressional election, Driehaus moved to withdraw the complaint and the Commission granted the motion with SBA's consent.[72]

SBA then filed suit in federal district court challenging the constitutionality of the statute on First Amendment grounds, alleging that the statute chilled and burdened its right to comment on election candidates and that it planned to make similar comments in future elections.[73] The district court dismissed SBA's suit and a similar suit by another organization as non-justiciable, concluding that neither suit presented a sufficiently concrete injury for purposes of standing or ripeness.[74] The Sixth Circuit affirmed on ripeness grounds.[75] The Supreme Court granted certiorari and reversed, holding that SBA had Article III standing to sue.[76]

In *Susan B. Anthony*, the Court treated both tests in *Clapper* as valid, stating: "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur.'"[77] The *Susan B. Anthony* decision appeared to rely on the substantial risk test in concluding that "the threat of future enforcement of the false statement statute [was] substantial."[78] The *Susan B. Anthony* decision cited

69 *Id.*

70 *Id.* at 2339–40.

71 *Id.*

72 *Id.* at 2340.

73 *Id.* The district court consolidated SBA's suit with a separate suit brought by petitioner Coalition Opposed to Additional Spending and Taxes, an advocacy organization that also alleged that the same Ohio false statement provisions are unconstitutional both facially and as applied. *Id.*

74 *Id.* (citing Susan B. Anthony List v. Driehaus, 525 Fed. App'x 415, 420–22 (6th Cir. 2013), *rev'd*, 134 S. Ct. 2334 (2014)).

75 *Id.* at 2340–41 (discussing *Susan B. Anthony*, 525 Fed. App'x at 420–22).

76 *Id.* at 2338, 2341, 2343–47.

77 *Id.* at 2341 (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5. (2013)); *see also* MadStad Eng'g, Inc. v. U.S. Patent & Trademark Office, 756 F.3d 1366, 1380 (Fed. Cir. 2014) ("This sentence [from *Susan B. Anthony*] seems to support MadStad's argument that there is a separate 'substantial risk' test that survived *Clapper* and that the district court should have considered. We need not decide whether these are alternative tests for standing applicable to all factual circumstances, however."); Chevron Corp. v. Donziger, 974 F. Supp. 2d 362, 554 n.1257 (S.D.N.Y. 2014) ("*Clapper* acknowledged that the 'substantial risk' and 'clearly impending' standards may be coextensive and, even if they are not, did not abandon the former." (citing *Clapper*, 133 S. Ct. at 1130 n.5)).

78 *Susan B. Anthony*, 134 S. Ct. at 2345; *see also* Lederman, *supra* note 56 ("*Susan B. Anthony* does appear to indicate that it is footnote 5 of *Clapper*—rather than the broader statements in that case about the need for plaintiffs to demonstrate 'certainly impending' harm—that will generally govern Article III standing doctrine going forward.").

Clapper as providing mild indirect support, indicating that readers should compare the case for its conclusion that the Ohio Election Commission's prior enforcement against the organization implied a substantial risk of future enforcement.[79]

The Court held that SBA met the Article III injury requirement because the organization faced a "credible" threat of enforcement by the Commission in future elections.[80] The Court concluded it was likely that SBA would accuse candidates in future elections of supporting "taxpayer-funded abortion" and that the Commission would conclude that such statements violated Ohio's broad false-statement law.[81] The Court concluded that the risk of future enforcement against SBA was substantial because of past enforcement actions against SBA, the fact that a majority of the Commission had already found "probable cause" that SBA had violated the statute,[82] because "any person" may file a complaint,[83] because the Commission hears "about 20 to 80 false-statement complaints per year,"[84] and because the burden of facing a hearing may chill free speech even if there is no conviction.[85] Furthermore, the Court held that "burdensome Commission proceedings here are backed by the additional threat of criminal prosecution. We conclude that the combination of those two threats suffices to create an Article III injury under the circumstances of this case."[86] While data breach cases involve significantly different facts and policy considerations than the threat of prosecution in *Susan B. Anthony*, the willingness of the Court in that case to apply a more

79 As the Court noted:

> We have observed that past enforcement against the same conduct is good evidence that the threat of enforcement is not "chimerical." [In *Clapper*,] plaintiffs' theory of standing was "substantially undermine[d]" by their "fail[ure] to offer any evidence that their communications ha[d] been monitored" under the challenged statute[ ]. Here, the threat is even more substantial given that the Commission panel actually found probable cause to believe that SBA's speech violated the false statement statute.

Susan B. Anthony, 134 S. Ct. at 2345 (second, third, and fourth alterations in original) (internal quotation marks omitted) (citations omitted) (first quoting Steffel v. Thompson, 415 U.S. 452, 459 (1974); and then quoting *Clapper*, 133 S. Ct. at 1148).

80 *Id.* at 2343–46.

81 *Id.*

82 *Id.* at 2345.

83 *Id.* (quoting OHIO REV. CODE ANN. § 3517.153(A) (West 2016)).

84 *Id.* (quoting Brief for Petitioners at 46, *Susan B. Anthony*, 134 S. Ct. 2334 (No. 13-193)).

85 *Id.* at 234–46.

86 *Id.* at 2346 (citing Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 302 n.1 (1979)). Subsequently, on remand, the U.S. District Court for the Southern District of Ohio held that Ohio's political false-statements laws violated the First Amendment's protections for political speech. Susan B. Anthony List v. Ohio Election Comm'n, 45 F. Supp. 3d 765, 770 (S.D. Ohio 2014); *see also* Rick Hasen, *Breaking: Federal Court Strikes Down Ohio False Campaign Speech Statute: Analysis*, ELECTION LAW BLOG (Sept. 11, 2014, 2:09 PM), http://electionlawblog.org/?p=65323 (analyzing the district court decision holding that Ohio's political false-statement laws violate the First Amendment).

lenient standing standard for future injuries than *Clapper*'s "certainly impending" test provides at least some argument for a more lenient standard in data breach cases where there is an increased potential for future identity theft because of the breach but no actual harm at the time a suit is filed.[87]

III. IDENTITY THEFT AND CREDIT FRAUD CASES BEFORE AND AFTER *CLAPPER*

A. Cases Allowing Standing Before Clapper

1. The Seventh Circuit in *Pisciotta v. Old National Bancorp*

In 2007, in *Pisciotta v. Old National Bancorp*,[88] the Seventh Circuit in a data breach case involving a defendant bank held that the plaintiffs' allegations of a threat of future harm from the breach were sufficient to confer Article III standing.[89] However, the Seventh Circuit also held that the plaintiffs' breach of contract and negligence actions, seeking recovery of the costs of credit monitoring services pursuant to Indiana law, must fail in the absence of present, actual damages.[90] The Seventh Circuit's decision in *Pisciotta* demonstrates that there is no guarantee in data breach cases that a plaintiff will win on the merits even if successful on the preliminary jurisdictional issue of Article III standing.[91]

The *Pisciotta* decision's discussion of standing was brief. The Seventh Circuit acknowledged, and cited in a footnote, four federal district court decisions from different jurisdictions, including two unpublished decisions, that had in 2006 or in 2007 denied Article III standing in data breach cases on the grounds that a mere breach of a computer system without actual harm was an insufficient injury for Article III standing.[92] The Seventh Circuit disagreed with those decisions, stating: "As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[93] In footnote three, the *Pisciotta* decision cited decisions from the Second, Fourth, Sixth, and Ninth Circuits that recognized standing for possible future injuries from exposure to toxic substances or defective medical implements.[94] In footnote four, the *Pisciotta* decision cited three prior Seventh Circuit decisions that held that a future risk of harm is sufficient to establish a cognizable injury for standing purposes as long as the probability of injury is more than hypothetical.[95] Based on the cases it cited

87 *See infra* Section III.D, Conclusion.
88 499 F.3d 629 (7th Cir. 2007).
89 *Id.* at 634; *see also* Jacobus & Watson, *supra* note 6, at 17, 21–22 (discussing *Pisciotta*).
90 *Pisciotta*, 499 F.3d at 634–40.
91 *See id.*
92 *Id.* at 634 & n.2.
93 *Id.* at 634.
94 *Id.* at 634 n.3.
95 *Id.* at 634 n.4.

in footnotes three and four, the Seventh Circuit's decision in *Pisciotta* implied that plaintiffs in data breach cases could establish standing if there was at least a small probability that the breach could cause future injury.[96] After the *Clapper* decision, district courts in the Seventh Circuit have disagreed whether *Pisciotta*'s liberal approach to standing in data breach cases is still valid;[97] the Seventh Circuit, in its *Remijas* decision, recognized standing in a data breach case, but did not directly address whether the *Pisciotta* decision is still good law.[98]

2. The Sixth Circuit in *Beaudry v. Telecheck Services, Inc.*

In 2009, in *Beaudry v. Telecheck Services, Inc.*,[99] the Sixth Circuit, in an opinion by Judge Jeffrey Sutton, held that a plaintiff had standing to bring a claim against defendants, which provided check verification services for willful violations of the FCRA,[100] even though she could not prove she had suffered any consequential damages, because the statute establishes statutory damages for willful violations.[101] The plaintiff in her complaint alleged that the defendants willfully violated her rights under the FCRA because they failed to address a change in the numbering system used by the Tennessee state driver's license system, and, as a result, erroneously reported the plaintiff as a first-time check-writer when businesses used the defendants' check verification services to determine the worthiness of the plaintiff's checks.[102] The district court granted the defendants' motion to dismiss the case on the grounds that the plaintiff had not proven an injury, but the Sixth Circuit reversed the dismissal of the case on the grounds that the alleged willful violation of her statutory rights pursuant to the FCRA was an injury sufficient to

96 *See id.* at 634 nn. 3–4.

97 *Compare* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014) ("I respectfully disagree with my colleagues that *Clapper* should be read to overrule *Pisciotta*'s holding that an elevated risk of identity theft is a cognizable injury-in-fact."), *with* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878–79 (N.D. Ill. 2014) ("*Clapper* seems rather plainly to reject the premise, implicit in *Pisciotta* . . . that any marginal increase in risk is sufficient to confer standing. . . . It is difficult . . . to reconcile . . . the Court's emphatic reiteration of the 'certainly impending' standard, with the Seventh Circuit's seeming view in *Pisciotta* that any risk of future harm suffices to confer standing. . . . To the extent that *Pisciotta* stands for the proposition that a risk of future harm does not have to be 'imminent,' 'certainly impending,' or pose greater than an objectively reasonable likelihood of injury (the standard *Clapper* expressly rejected as inadequate), this Court cannot square it with *Clapper*." (footnote omitted)). *See generally* Jacobus & Watson, *supra* note 6, at 31–32, 53–55, 57–58, 60–61, 64, 66 (discussing the split in lower court decisions as to whether *Pisciotta* remains good law after the *Clapper* decision).

98 *Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 692–97 (7th Cir. 2015); *see also infra* subsection III.D.3.

99 579 F.3d 702 (6th Cir. 2009).

100 15 U.S.C. §§ 1681e(b), 1681n(a) (2012).

101 *Beaudry*, 579 F.3d at 703, 705–08.

102 *Id.* at 703–05. She also tried to file the suit as a class action for other Tennessean consumers. *Id.*

establish standing and to defeat the defendants' motion to dismiss under Federal Rule of Civil Procedure 12(b)(6).[103]

Because the plaintiff alleged that the defendants violated her personal statutory rights, Judge Sutton concluded that she had met Article III's injury requirement for standing because Congress has considerable discretion in defining statutory injury as long as a plaintiff alleges an individual rather than a collective injury, as was recognized by the Supreme Court's *Havens Realty Corp. v. Coleman* decision.[104] As will be discussed in Section III.D, some subsequent decisions have also relied on the statutory standing principles in the Court's *Havens Realty Corp.* decision to justify a statutory standing injury despite the absence of actual damages as an exception to the "certainly impending" standard in *Clapper*.[105] The *Beaudry* decision is most useful as a precedent for plaintiffs alleging willful violations by a defendant of a federal statutory right, as opposed to those raising state common law claims.

3. The Ninth Circuit in *Krottner v. Starbucks Corp.*

In 2010, in *Krottner v. Starbucks Corp.*,[106] the Ninth Circuit held that the plaintiffs' allegation that the theft of a laptop from their employer subjected them to increased risk of future identity theft was sufficient to establish injury-in-fact for purposes of Article III standing.[107] In 2008, someone stole a laptop from Starbucks Corporation (Starbucks).[108] The laptop contained the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees.[109] Starbucks sent a letter to each of its affected employees alerting them to the potential danger of identity theft and offering to pay for one year of credit monitoring.[110]

Several current and former Starbucks employees whose personal information was stored on the stolen laptop sued Starbucks, alleging that it acted negligently and breached an implied contract under state law in failing to protect their personal data.[111] The district court concluded that the plaintiffs' alleged injuries met Article III standing requirements, but on the merits granted Starbucks's motion to dismiss on the grounds that the plaintiffs failed to allege a cognizable injury under state law.[112] On appeal, the Ninth Circuit affirmed both the district court's conclusion that the plaintiffs met

103 *Id.* at 703–08.

104 *Id.* at 707–09 (citing Havens Realty Corp. v. Coleman, 455 U.S. 363, 373 (1982)).

105 *See infra* Section III.D.

106 628 F.3d 1139 (9th Cir. 2010).

107 *Id.* at 1140–43; *see also* Jacobus & Watson, *supra* note 6, at 22–23 (discussing *Krottner*).

108 *Krottner*, 628 F.3d at 1140.

109 *Id.* at 1140.

110 *Id.* at 1140–41.

111 *Id.*

112 *Id.*

Article III standing requirements and its dismissal of the suit on the merits.[113]

Because the defendant did not dispute standing causation or redressability, the Ninth Circuit focused on whether the plaintiffs had alleged a sufficient injury for Article III standing.[114] Initially, the court determined that plaintiff Lalli's allegation that he "has generalized anxiety and stress" as a result of the laptop theft constituted the only present injury asserted by any of the plaintiffs, and that all the other allegations addressed potential future injuries from identity theft.[115] The Ninth Circuit concluded that Lalli's allegations of present emotional distress were sufficient for standing because the Supreme Court's 2004 decision in *Doe v. Chao*[116] had suggested that allegations of similar emotional distress were sufficient for Article III standing, but were insufficient to win damages under the Federal Privacy Act.[117]

Next, the Ninth Circuit addressed whether the plaintiffs' allegations of increased risk of future identity theft were sufficient to establish injury for Article III standing.[118] The court observed that several environmental cases or cases seeking medical monitoring expenses after plaintiffs were exposed to toxic substances had recognized standing for potential future injuries.[119] The Seventh Circuit in *Pisciotta* relied on these environmental and medical monitoring cases to allow standing for plaintiffs alleging that they are at an increased risk of future identity theft as a result of a data breach of a defendant's computers.[120] On the other hand, the Sixth Circuit in *Lambert v. Hartman*[121] recognized standing where a plaintiff suffered actual financial loss and the thief acknowledged obtaining the plaintiff's personal data from a government website, but had, according to the Ninth Circuit's interpretation of the case, "noted, without analysis, that the risk of future identity theft was somewhat 'hypothetical' and 'conjectural.'"[122] The Ninth Circuit in *Krottner* disagreed with the *Lambert* decision's view that the risk of future identity theft was "somewhat 'hypothetical' and 'conjectural,'" and instead agreed with the approach in the *Pisciotta* decision that the plaintiffs "have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[123] Accordingly, the Ninth Circuit held that the plaintiffs' allegations of potential future harm from identity theft as a result of the data breach were sufficient injury for Article III stand-

113 *Id.* at 1140–43.

114 *Id.* at 1141–43.

115 *Id.* at 1142.

116 540 U.S. 614 (2004).

117 *Krottner*, 628 F.3d at 1142 (citing *Chao*, 540 U.S. at 617–18, 624–25).

118 *Id.* at 1142–43.

119 *Id.* at 1142.

120 *Id.* at 1142–43.

121 517 F.3d 433 (6th Cir. 2008).

122 *Krottner*, 628 F.3d at 1143 (internal quotation marks omitted) (quoting *Lambert*, 517 F.3d at 437).

123 *Id.*

ing.[124] As will be discussed in Section III.D, courts in the Ninth Circuit have continued to apply the liberal approach to standing in data breach cases employed in *Krottner* even after the *Clapper* decision.[125] However, lower courts in other circuits have questioned the continuing validity of *Krottner* in light of the *Clapper* decision.[126]

B. Cases Denying Standing Before Clapper

Before the *Clapper* decision, the most important case to deny standing in a data breach case was the Third Circuit's 2011 decision in *Reilly v. Ceridian*.[127] In *Reilly*, two law firm employees brought a putative class action against a payroll processing firm, the defendant Ceridian Corporation, after a hacker breached Ceridian's computer system and gained access to the personal and financial data of 27,000 employees at 1900 companies, including the plaintiffs' information.[128] It is unknown whether the hacker used any of the data.[129] Ceridian sent letters to the potential identity theft victims informing them of the breach, and offered to provide the potentially affected individuals with one year of free credit monitoring and identity theft protection.[130]

The plaintiffs filed suit, on behalf of themselves and all others similarly situated, alleging various claims, including negligence and breach of contract, related to an increased risk of identity theft and incurred costs to monitor credit activity, as well as a claim for emotional distress.[131] The district court dismissed the plaintiffs' claims for lack of standing and also for failure to state a claim on the merits because they failed to adequately allege the damage, injury, and ascertainable loss elements of their claims.[132] On appeal, the Third Circuit affirmed the decision of the district court on the sole ground that the plaintiffs' "allegations of hypothetical, future injury do not establish standing under Article III."[133]

The Third Circuit quoted the Supreme Court's 1990 decision in *Whitmore v. Arkansas* for the principle that allegations of future injury are sufficient for the injury-in-fact requirement of Article III standing only if those threatened injuries are "certainly impending" and imminent, so as to avoid

124 *Id.*

125 *See, e.g.*, *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1212–14 (N.D. Cal. 2014) (arguing the *Krottner* decision is consistent with the *Clapper* decision); *see also* Jacobus & Watson, *supra* note 6, at 26, 58, 64 (discussing Ninth Circuit cases following the *Krottner* decision); *infra* Section III.D.

126 *See* Jacobus & Watson, *supra* note 6, at 55–56 (discussing lower court decisions outside the Ninth Circuit cases questioning the *Krottner* decision); *infra* Section III.C.

127 664 F.3d 38 (3rd Cir. 2011); *see also* Jacobus & Watson, *supra* note 6, at 23–24 (discussing *Reilly*).

128 *Reilly*, 664 F.3d at 40.

129 *Id.*

130 *Id.*

131 *Id.*

132 *Id.* at 41.

133 *Id.* at 41–46.

suits based on speculative or hypothetical harms.[134] The subsequent *Clapper* decision also relied on *Whitmore* in making the "certainly impending" standard the key to whether a future injury is sufficient for Article III standing,[135] but in a footnote the *Clapper* majority opinion acknowledged that the Court had sometimes used a less stringent "substantial risk" standard,[136] and Justice Breyer's dissenting opinion demonstrated that the Court in several cases had used a less stringent standard.[137] Thus, the Third Circuit's reliance on the "certainly impending" standard was a possible reading of the Supreme Court's precedent on when allegations of future injury are sufficient for Article III standing, but the Court's standing doctrine regarding that question is far more complicated than that standard.[138]

In *Reilly*, the Third Circuit concluded that the plaintiffs' allegations regarding potential future identity theft were mere "speculation."[139] The court stated, "Unless and until these conjectures [of the hacker using the plaintiffs' personal information to their detriment by making unauthorized transactions in their names] come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm."[140] The *Reilly* decision emphasized that the plaintiffs' "alleged increased risk of future injury is even more attenuated, because it is dependent on entirely speculative, future actions of an unknown third-party."[141]

The Third Circuit distinguished the situations in both the Seventh Circuit's decision in *Pisciotta* and the Ninth Circuit's decision in *Krottner* as involving significantly greater risk of future harm than the facts in the *Reilly* case.[142] The Third Circuit stated:

> [I]n *Pisciotta* and *Krottner*, the threatened harms were significantly more "imminent" and "certainly impending" than the alleged harm here. In *Pisciotta*, there was evidence that "the [hacker's] intrusion was sophisticated, intentional and malicious." In *Krottner*, someone attempted to open a bank account with a plaintiff's information following the physical theft of the laptop. Here, there is no evidence that the intrusion was intentional or malicious. Appellants have alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was pene-

134 *Id.* at 42 (internal quotation marks omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

135 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143, 1147–48 (2013) (quoting *Whitmore*, 495 U.S. at 157–60).

136 *Id.* at 1150 n.5; *see also* Mank, *Two or Three*, *supra* note *, at 221, 230–31, 236–37 (discussing the "substantial risk" test in footnote 5 of *Clapper*).

137 *Clapper*, 133 S. Ct. at 1160–65 (Breyer, J., dissenting); *see also* Mank, *Two or Three*, *supra* note *, at 236–39 (discussing Breyer's dissenting opinion in *Clapper*).

138 *See also* Mank, *Two or Three*, *supra* note *, at 221, 230–31, 236–39, 269, 275 (discussing the Supreme Court's use of standards other than *Clapper*'s "certainly impending" test in deciding when allegations of future injury are sufficient for Article III standing).

139 *Reilly*, 664 F.3d at 42–43.

140 *Id.* at 42.

141 *Id.*

142 *Id.* at 43–44; *see also* Jacobus & Watson, *supra* note 6, at 23–24 (discussing how *Reilly* distinguished the *Pisciotta* and *Krottner* decisions).

> trated. Appellants' string of hypothetical injuries do not meet the requirement of an "actual or imminent" injury.[143]

Additionally, the Third Circuit criticized both the *Pisciotta* and the *Krottner* decisions for failing to apply the correct constitutional standing test requiring an "imminent" and "certainly impending" risk of future injury.[144] The *Reilly* decision stated:

> Neither *Pisciotta* nor *Krottner*, moreover, discussed the constitutional standing requirements and how they apply to generalized data theft situations. Indeed, the *Pisciotta* court did not mention—let alone discuss—the requirement that a threatened injury must be "imminent" and "certainly impending" to confer standing. Instead of making a determination as to whether the alleged injury was "certainly impending," both courts simply analogized data-security-breach situations to defective-medical-device, toxic-substance-exposure, or environmental-injury cases.[145]

The Third Circuit argued that the defective-medical-device, toxic-substance-exposure, or environmental-injury cases relied on by both the *Pisciotta* and *Krottner* decisions were not good analogies to mere data breaches because the former cases involved actual or quantifiable risks of serious harms to the human health or the environment that often cannot be adequately compensated through monetary damages because human health or environmental habitat, once damaged, may never be perfectly restored.[146] By contrast, the plaintiffs in *Reilly* merely speculated that a hacker might cause unquantifiable future financial losses.[147] Anticipating the approach in the subsequent *Clapper* decision, the Third Circuit concluded that the plaintiffs' expenditures on preventative measures such as credit monitoring could not be used to establish standing when the plaintiffs could not prove that they would suffer future injuries as a result of the actions of the defendants;[148] similarly, the *Clapper* decision held that the plaintiffs' expenditure of travel monies to avoid electronic surveillance by the government could not establish standing injury when the plaintiffs could not prove the government was actually spying on them but merely speculated that spying might occur.[149] Accordingly, the *Reilly* decision held that the plaintiffs failed to prove standing injury and dismissed their case.[150] The Third Circuit's approach to standing, requiring an "imminent" and "certainly impending" risk of future injury, was far narrower than either the *Pisciotta* or *Krottner*

143 *Reilly*, 664 F.3d at 44 (second alteration in original) (footnote omitted) (citations omitted) (quoting Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007)).

144 *Id.* at 44–46.

145 *Id.* at 44 (citations omitted).

146 *Id.* at 44–46; *see also* Jacobus & Watson, *supra* note 6, at 23–24 (discussing how *Reilly* questioned the standing analysis in the *Pisciotta* and *Krottner* decisions).

147 *Reilly*, 664 F.3d at 45.

148 *Id.* at 46.

149 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150–53 (2013); *see also* Mank, *Two or Three*, *supra* note *, at 231–32.

150 *Reilly*, 664 F.3d at 46.

decisions, but the *Reilly* decision left open the possibility that some instances of data breach involving evidence of intentional or malicious intrusion could meet the Article III standing test.[151]

C. Cases Denying Standing After Clapper

1. The Southern District of Ohio in *Galaria v. Nationwide Mutual Insurance Co.*

Some lower court decisions have interpreted the *Clapper* decision's "certainly impending" standard to bar data breach suits where there is no proof of actual injury from the breach and there is only an increased risk of future injury.[152] In *Galaria v. Nationwide Mutual Insurance Co.*,[153] consumers brought related putative class actions in the federal district court for the Southern District of Ohio against defendant insurer Nationwide Mutual Insurance Company, alleging violations of the FCRA, negligence, invasion of privacy, and bailment, stemming from a third party hacker's theft of the plaintiffs' personally identifiable information (PII) from the insurer's computer network.[154] The defendant had sent a letter to the plaintiffs alerting them to the data breach and offering them one year of free credit monitoring and identity theft protection.[155] Additionally, the defendant suggested that the plaintiffs place a security freeze on their credit reports at their own expense.[156] Neither of the two named plaintiffs alleged that his personal information was misused or that his identity was stolen as a result of the data breach.[157]

Judge Michael H. Watson's opinion emphasized the *Clapper* decision's "certainly impending" standard in concluding that the plaintiffs' allegations that they were at an increased risk of future identity theft was insufficient to establish a standing injury because *Clapper* had rejected "similar" allegations by the plaintiffs in that case (that they were at an increased risk of future government surveillance because of the types of clients that they represented) as insufficient to demonstrate standing injury.[158] The *Galaria* district court stated:

---

151 *Id.* at 42–46.

152 *See generally* Jacobus & Watson, *supra* note 6, at 50–61 (arguing that many, but not all, lower court decisions applying *Clapper*'s "certainly impending" test in data breach cases have required more evidence of imminent harm from the breach than many pre-*Clapper* decisions).

153 998 F. Supp. 2d 646 (S.D. Ohio 2014), *rev'd*, Nos. 15-3386/3387, 2016 WL 4728027 (6th Cir. Sept. 12, 2016).

154 *Id.* at 646.

155 *Id.* at 650.

156 *Id.*

157 *Id.*

158 *Id.* at 651, 654–56 (discussing the *Clapper* decision's "certainly impending" standard); *see also* Jacobus & Watson, *supra* note 6, at 54–55, 59–60 (observing that the *Galaria* decision interpreted *Clapper* to reject standing based solely upon an increased risk of future identity theft).

> In this case, an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—or offer facts to make plausible—an allegation that such harm is "certainly impending." Even though Plaintiffs alleged they are 9.5 times more likely than the general public to become victims of theft or fraud, that factual allegation sheds no light as to whether theft or fraud meets the "certainly impending" standard. That is, a factual allegation as to how much *more likely* they are to become victims than the general public is not the same as a factual allegation showing how likely they are to become victims.
>
> Other allegations in the Complaint show such harm is *not* certainly impending. For example, Named Plaintiffs state that consumers who receive a data breach notification had a fraud incidence rate of 19% in 2011. An injury can hardly be said to be "certainly impending" if there is less than a 20% chance of it occurring.[159]

Judge Watson also concluded that the plaintiffs' allegations of future injury were speculative because they depended upon the decisions of independent, third-party criminals outside the control of the defendant.[160]

Additionally, in a footnote, the *Galaria* district court concluded that a less-than-twenty-percent chance of identity theft was insufficient to meet the Supreme Court's alternative "substantial risk" standing test acknowledged by the *Clapper* decision.[161] Nor could the *Galaria* plaintiffs' alleged expenditures to avoid future identity theft establish standing injury: the *Clapper* decision rejected its plaintiffs' argument that their expenditures to avoid government surveillance could establish standing because "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[162] Finally, Judge Watson acknowledged decisions such as *Pisciotta* or *Krottner*, which found standing in data breach cases where there was only an increased risk of future injury, but he concluded that they were no longer good law in light of the subsequent *Clapper* decision's "certainly impending" standard.[163] Accordingly, because the plaintiffs' complaint did not sufficiently allege that their risk of future identity theft was "certainly impending," the *Galaria* district court held that the plaintiffs failed to establish an Article III standing injury for their common law claims.[164]

---

159 *Galaria*, 998 F. Supp. 2d at 654 (footnote omitted) (citation omitted).

160 *Id.* at 655. *But see In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014) (criticizing *Galaria*'s reasoning that it was uncertain whether third-party hackers would steal information from plaintiffs because "after all, why would hackers target and steal personal customer data if not to misuse it?").

161 *Galaria*, 998 F. Supp. 2d at 654 n.8.

162 *Id.* at 657 (internal quotation marks omitted) (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143, 1151 (rejecting respondents' alternative argument that they were suffering "*present* injury because the risk of . . . surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications")).

163 *Id.* at 656.

164 *Id.* at 658.

The *Galaria* plaintiffs also argued that they had statutory standing for their FCRA claims.[165] The FCRA's sections 1681n(a) and 1681*o* establish "causes of action for, respectively, the willful and negligent failure 'to comply with any requirement imposed under this subchapter.'"[166] Judge Watson concluded that the plaintiffs' vague allegations that the defendant should have employed more protective measures to prevent data breaches were insufficient because their complaint failed to allege a specific duty set forth in the FCRA that the defendant allegedly violated.[167] Thus, he concluded that the plaintiffs had failed to establish statutory standing for their FCRA claims.[168]

In 2016, the Sixth Circuit in a divided decision reversed and remanded for further proceedings the district court's decision in *Galaria*.[169] The court of appeals concluded that the district court had erred in dismissing the FCRA claims for lack of subject-matter jurisdiction.[170] Disagreeing with the district court's conclusion that the plaintiffs had failed to demonstrate a "substantial risk" of identity theft because that risk was less than twenty percent,[171] the Sixth Circuit concluded that the plaintiffs had alleged a substantial risk of fraud and identity theft because "their data has already been stolen and is now in the hands of ill-intentioned criminals."[172] While acknowledging that it was not certain that criminals would misuse the plaintiffs' stolen personal data, the court of appeals determined that the failure of Nationwide to pay for a "security freeze" that the defendant had recommended to the plaintiffs established that the plaintiffs had suffered a concrete and unmitigated injury sufficient for Article III standing.[173]

The Sixth Circuit reasoned that its conclusion was "in line" with the Seventh Circuit's decision in *Remijas* and the Ninth Circuit's decision in *Kottner*, although inconsistent with the Third Circuit's *Reilly* decision.[174] However, the Sixth Circuit's conclusion that victims of a data breach suffer a substantial injury from the breach alone without any actual misuse of the data is arguably broader than the Seventh Circuit's decision in *Remijas* where 9200 customers had already suffered actual fraudulent uses of their credit cards or bank accounts.[175] The Sixth Circuit in *Galaria* tried to align itself with the *Remijas* decision by quoting language from the Seventh Circuit's decision that hackers presumably steal private information for the purpose of eventu-

165 *Id.* at 652.

166 *Id.* (quoting 15 U.S.C. §§ 1681n(a), 1681*o* (2012)).

167 *Id.* at 653.

168 *Id.*

169 Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 2016 WL 4728027, at *1, *6 (6th Cir. Sept. 12, 2016).

170 *Id.*

171 *Galaria*, 998 F. Supp. 2d at 654 n.8.

172 *Galaria*, 2016 WL 4728027, at *3.

173 *Id.*

174 *Id.* at 4.

175 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690, 692-93 (7th Cir. 2015).

ally committing fraud.[176] The Seventh Circuit in *Remijas* used the actual misuse of 9200 customers' data to establish that there was indeed a substantial risk of intentional hacking and fraud, but did not squarely address whether a data breach alone is sufficient for Article III standing.[177]

In her dissenting opinion, Judge Alice M. Batchelder "disagree[d] with the majority's conclusion that the complaints have adequately pled a causal connection between Nationwide's alleged inaction and the plaintiffs' alleged injury."[178] She reasoned that it was unnecessary for her to address the split in the circuits regarding whether an increased risk of identity theft is an Article III injury because she concluded that the plaintiffs had failed to establish the second prong of Article III standing, whether there was a causal connection between the defendants' actions and the plaintiffs' injuries.[179] Judge Batchelder argued that the plaintiffs could not simply allege that Nationwide's lax security measures allowed the hackers to access the plaintiffs' private data, but must specifically explain what measures Nationwide could have used to prevent the breach and whether the defendant failed to use such preventative measures.[180] She disagreed with the reasoning of *Remijas* and other decisions holding defendants liable for data breaches because they "completely ignore[d] the independent third party criminal action breaking the chain of causation."[181] Her focus on the issue of standing causation rather than on whether there was a sufficient injury for Article III standing is quite different from the overwhelming majority of cases discussed in this Article.[182]

Because defendants are in a better position to know whether they could have prevented a data breach than plaintiffs, it is unfair to adopt Judge Batchelder's approach of placing the burden on the plaintiffs to explain what measures the defendant should have used to prevent the breach, in order to establish standing causation. In *Remijas*, the Seventh Circuit appropriately reasoned that a plaintiff may establish standing causation by providing plausible evidence that a defendant's actions harmed the plaintiff and that a defendant may, at trial, show that other data breaches actually caused the harm to the plaintiff.[183] Furthermore, courts might allow defendants to make an affirmative defense on the merits: that they used all reasonable measures to prevent the data breach.

176 *Galaria*, 2016 WL 4728027, at *4.

177 *See Remijas*, 794 F.3d at 692-96; subsection III.D.3.

178 *Galaria*, 2016 WL 4728027, at *6 (Batchelder, J., dissenting).

179 *Id.*

180 *Id.* at *7–8.

181 *Id.* at *8.

182 *Compare id.* at *6–8, *with* Part III (discussing several cases focusing on the issue of whether a data breach poses a sufficient Article III standing injury).

183 *Remijas*, 794 F.3d at 696.

2. The Decision of the U.S. District Court for the District of Columbia Regarding *In re: Science Applications International Corp. Backup Tape Data Theft Litigation*

Agreeing with the *Galaria* decision, the U.S. District Court for the District of Columbia concluded in its case *In re: Science Applications International Corp. Backup Tape Data Theft Litigation* (*SAIC*)[184] that the risk of identity theft alone is insufficient to establish an injury in fact sufficient for Article III standing in light of the *Clapper* decision's "certainly impending" standard or even its alternative "substantial risk" test.[185] In *SAIC*, a thief broke into a car and stole several data tapes.[186] The tapes belonged to an employee of Science Applications International Corporation, an information-technology company that handles data for the federal government.[187] The tapes contained personal information and medical records concerning 4.7 million members of the U.S. military and their families who were enrolled in TRICARE healthcare.[188]

SAIC mailed letters to the service members affected by the data breach.[189] SAIC offered all affected members one year of free credit monitoring and identity theft protection.[190] Additionally, SAIC, in its letter, argued that the risk that any "information could be obtained from these tapes is low since accessing, viewing and using the data requires specific hardware and software."[191]

The plaintiffs filed several lawsuits in various courts around the country alleging injury from an increased likelihood of identity theft from the data breach and from an invasion of their privacy, among other claims.[192] Eight of those suits were consolidated in the U.S. District Court for the District of Columbia as a multidistrict litigation.[193] Judge James E. Boasberg concluded that two of the plaintiffs had made "plausible" assertions that their data was accessed or abused, and could move forward with their claims; however, he observed that these two plaintiffs would have to prove that the alleged abuse occurred as a result of the theft of the SAIC tapes and that there was a significant possibility that the court might ultimately decide on the merits that the alleged abuse was the result of unrelated data breaches or identity theft.[194]

---

184 45 F. Supp. 3d 14 (D.D.C. 2014).

185 *Id.* at 24–28; *see also* Jacobus & Watson, *supra* note 6, at 55–56, 59–60 (observing that the *SAIC* decision interpreted *Clapper* to reject standing based solely upon an increased risk of future identity theft).

186 *SAIC*, 45 F. Supp. 3d at 19.

187 *Id.*

188 *Id.*

189 *Id.* at 20.

190 *Id.*

191 *Id.*

192 *Id.* at 19.

193 *Id.*

194 *Id.* at 19, 33–34.

Next, the *SAIC* decision addressed whether the plaintiffs, who simply asserted that they were at an increased risk of future identity theft as a result of the theft of the SAIC tapes, could establish a sufficient injury for Article III standing. Agreeing with the *Galaria* decision and similar district court decisions from around the nation, Judge Boasberg concluded that the plaintiffs' assertion that they were at a nineteen-percent risk of future identity theft was insufficient to meet the *Clapper* decision's "certainly impending" standard or even its alternative "substantial risk" test.[195] Furthermore, the *SAIC* decision agreed with the *Galaria* decision that decisions prior to the *Clapper* decision that had found standing based on a mere increased risk of identity theft stemming from a data breach were no longer viable.[196] Accordingly, Judge Boasberg held that those plaintiffs who simply asserted that they were at an increased risk of future identity theft as a result of the theft of the SAIC tapes could not establish a sufficient injury for Article III standing.[197]

D. Cases Allowing Standing After Clapper

1. The Southern District of California Decision *In re Sony Gaming Networks & Customer Data Security Breach Litigation*

Some lower courts have rejected the argument that the *Clapper* decision's "certainly impending" standard effectively bars standing for plaintiffs who are the victims of a data breach, but who can only allege the possibility of future harms from potential identity theft.[198] The U.S. District Court for the Southern District of California concluded in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*[199] that the *Clapper* decision did not change the "credible threat" test used by the Ninth Circuit in *Krottner* in concluding that victims of data breaches have suffered a cognizable injury for

195 *Id.* at 26–28 (first citing Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014); then citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C 2007); then citing Whitaker v. Health Net of Cal., Inc., No. 11-910, 2012 WL 174961 (E.D. Cal. Jan. 20, 2012); then citing Hammond v. Bank of N.Y. Mellon Corp., No. 08-6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010); then citing Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010); then citing Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009); then citing Bell v. Acxiom Corp., No. 06-485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); then citing Key v. DSW, Inc., 454 F.Supp.2d 684 (S.D. Ohio 2006); and then citing Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036 (D.N.J. July 31, 2006)).

196 *Id.* at 28 ("Yet after *Clapper*, *Gap III*'s 'credible threat of harm' standard [for proving 'actual injury for standing purposes'] is clearly not supportable." (quoting Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) (*Gap III*))).

197 *Id.* ("In sum, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm.").

198 *See* Jacobus & Watson, *supra* note 6, at 57–58, 59, 61, 66–67 (observing that a minority of lower court decisions interpreting *Clapper*'s "certainly impending" test in data breach cases have disagreed that it necessarily forecloses success by plaintiffs).

199 996 F. Supp. 2d 942 (S.D. Cal. 2014).

Article III standing.[200] The plaintiffs, a nationwide putative consumer class, alleged that three related online gaming companies owned by defendant Sony failed to provide reasonable network security, including utilizing industry-standard encryption, to safeguard their personal and financial information stored on Sony's network.[201] Third-party hackers accessed Sony's network and obtained the personal information of millions of Sony's customers, including the named plaintiffs.[202] Sony announced that it would compensate its users in the United States with free identity theft protection services and certain free downloads and online services, and would consider helping customers who had to apply for new credit cards.[203]

After different plaintiffs filed similar suits against defendant Sony in various district courts around the country, the Judicial Panel on Multidistrict Litigation transferred certain civil actions from these district courts into one consolidated action before the U.S. District Court for the Southern District of California.[204] Judge Anthony J. Battaglia denied Sony's motion to dismiss the case for lack of standing, but Sony requested that the district court reconsider its decision in light of the Supreme Court's recent *Clapper* decision.[205] Upon reconsideration, the district court concluded that the *Clapper* decision did not overrule the test used by the Ninth Circuit in *Krottner* in holding that victims of data breaches have suffered a cognizable injury for Article III standing. Judge Battaglia reasoned:

> [A]lthough the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be "certainly impending," rather than "real and immediate," the Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be "real and immediate."[206]

The *Sony* decision relied on several district court decisions in the Ninth Circuit that had followed *Krottner* in holding that a plaintiff whose personal information is wrongfully disclosed by a data breach has an Article III injury sufficient to sue a defendant who has failed to protect that information from a hacker or thief.[207] Applying a "credible threat" test, Judge Battaglia con-

200 *Id.* at 960–62; *see also* Jacobus & Watson, *supra* note 6, at 26, 51, 58, 64 (observing that the district court in *In re Sony* followed the Ninth Circuit's *Krottner* decision and distinguished *Clapper* as involving a less immediate threat than its facts).

201 *In re Sony*, 996 F. Supp. 2d at 953.

202 *Id.* at 955.

203 *Id.* Sony offered slightly different compensation depending upon with which of its three subsidiaries users did business. *Id.*

204 *Id.* at 956.

205 *Id.* at 956, 960.

206 *Id.* at 961.

207 *Id.* at 962 (first citing *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011); then citing Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102 (N.D. Cal 2010); and then citing San Luis & Delta-Mendota Water Auth. v. U.S. Dep't of the Interior, 905 F. Supp. 2d 1158 (E.D. Cal. 2012)).

cluded that the plaintiffs had established an Article III standing injury.[208] In a footnote, the *Sony* decision declined to follow the Third Circuit's contrary approach in *Reilly*—that data breaches unaccompanied by actual harm do not constitute a sufficient injury for Article III standing.[209]

2. Judge Elaine E. Bucklo's Decision in *Moyer v. Michaels Stores, Inc.*

Contrary to decisions by two other federal district court judges,[210] in the U.S. District Court for Northern Illinois, in *Moyer v. Michaels Stores, Inc.*,[211] Judge Elaine E. Bucklo "respectfully disagree[d] with [her] colleagues that *Clapper* should be read to overrule *Pisciotta*'s holding that an elevated risk of identity theft is a cognizable injury-in-fact."[212] She cited the *Sony* and *Krottner* decisions in support of her conclusion that an elevated risk of identity theft is sufficient for Article III standing.[213] In *Moyer*, six plaintiffs sued defendant Michaels Stores, Inc., an arts and crafts retailer, for failing to secure their credit and debit card information during in-store transactions.[214] The complaint asserted claims for breach of implied contract and violations of state consumer fraud statutes.[215] In a press release, Michaels acknowledged that there was some evidence that stolen credit card numbers, which had been obtained through malicious software ("malware") that had infected its point-of-sales systems, had been used in fraudulent transactions.[216] After seeing some evidence of misuse of credit card information, Michaels offered twelve months of identity protection, credit monitoring, and fraud assistance services to affected customers at no cost.[217] There was evidence that the credit card of Mary Whalen, a putative class member who sought to join the six plaintiffs, was used fraudulently, and the district court used her injury as evi-

208 *Id.*

209 *Id.* at 963 n.10.

210 *See* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("*Clapper* compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing." (citations omitted)); *In re* Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (Darrah, J.) (citing *Clapper* in support of the proposition that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing").

211 No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).

212 *Id.* at *5 (first citing *In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961–962 (S.D. Cal 2014); and then citing Krottner v. Starbucks, 628 F.3d 1139, 1142–43 (9th Cir. 2010)); *see also* Jacobus & Watson, *supra* note 6, at 57–58 (observing that the *Moyer* decision concluded that *Clapper* did not implicitly overrule standing analysis in *Pisciotta* based upon an increased risk of future identity theft, because other Supreme Court decisions applied a less strict standing approach than *Clapper*'s for allegations of future injury).

213 *Moyer*, 2014 WL 3511500, at *5.

214 *Id.* at *1.

215 *Id.*

216 *Id.* at *1–2.

217 *Id.* at *2.

dence that the six plaintiffs were at a heightened risk of an imminent injury from identity theft.[218]

Addressing the defendant's argument that the *Clapper* decision's stricter imminence requirement for plaintiffs seeking to establish standing based on a future risk of harm effectively abrogated the Seventh Circuit's decision in *Pisciotta*, which had recognized standing in data breach cases based on a heightened risk of identity theft, Judge Bucklo first interpreted *Clapper* as having adopted a strict interpretation of the imminence requirement for standing in the context of whether a national security statute was unconstitutional, and reasoned that "[t]he extent to which *Clapper*'s admittedly rigorous standing analysis should apply in a case that presents neither national security nor constitutional issues is an open question."[219] Second, she observed that the subsequent *Susan B. Anthony*[220] decision:

> catalogues the myriad circumstances in which a risk of future harm—such as enforcement of an allegedly unconstitutional law—has been deemed sufficiently imminent to establish Article III standing. The labels used to describe the imminence requirement in these cases—i.e., injury risks that are not "chimerical," "imaginary," or "wholly speculative" or, conversely, ones that are "credible" and "well-founded"—sound less demanding than *Clapper*'s rigorous application of the "certainly impending" standard.[221]

Based on "*Susan B. Anthony List* and the cases cited therein," Judge Bucklo concluded that the plaintiffs had introduced sufficient proof "that they face a credible, non-speculative risk of future harm. Although Plaintiffs cannot establish standing based solely on Whalen's injuries, the fraudulent charges she incurred within two weeks of shopping at Michaels informs my analysis of whether the risk of identity theft facing these Plaintiffs is substantial and well-founded."[222] Thus, Judge Bucklo used the harms allegedly suffered by a putative class plaintiff to substantiate an elevated risk of future injury for the six actual plaintiffs.[223]

Third, she relied upon the Supreme Court's decision in *Monsanto Co. v. Geertson Seed Farms*,[224] which recognized that the use of genetically engineered alfalfa gave rise to a "significant risk of gene flow to non-genetically-engineered varieties of alfalfa" on nearby organic farms, and which the *Clap-*

---

218 *Id.* at *2–6. But a district court in the Eastern District of New York dismissed Whalen's separate suit because she suffered no actual financial losses from fraudulent use of her credit card, and held there was no standing injury under *Clapper*'s "certainly impending" test. Whalen v. Michaels Stores, Inc., 153 F. Supp. 3d 577, 579–83 (E.D.N.Y. 2015).

219 *Moyer*, 2014 WL 3511500, at *5 (citing Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 n.11 (N.D. Ill. 2014)).

220 134 S. Ct. 2334 (2014).

221 *Moyer*, 2014 WL 3511500, at *5 (citations omitted) (first citing *Susan B. Anthony*, 134 S. Ct. at 2342–43; and then citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).

222 *Id.*

223 *Id.*

224 561 U.S. 139 (2010).

per decision quoted with approval.[225] Applying *Monsanto*'s significant risk test to the facts of her case, Judge Bucklo concluded:

> If a bee's anticipated pollination patterns create a sufficiently imminent risk of injury to alfalfa farmers who fear gene flow from genetically engineered plants in nearby fields, I fail to see how the transfer of information from a data hacker to an identity thief (assuming they are not one and the same) could be deemed an overly attenuated risk of harm.[226]

Accordingly, Judge Bucklo held that the plaintiffs' allegations that they were at an "elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing."[227] She explained her reasoning for finding standing as follows:

> This conclusion follows from *Pisciotta* and is consistent with a host of Supreme Court decisions finding standing based on an imminent risk of future injury. *Clapper* is distinguishable based on its admittedly rigorous application of the "certainly impending" standard in a case that involved (1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances.[228]

3. The Seventh Circuit Distinguishes *Clapper* in *Remijas v. Neiman Marcus Group, LLC*

During 2015, a three-judge panel of the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC* distinguished the *Clapper* decision in holding that plaintiffs whose personal data had been stolen from the defendant retailer had Article III standing to sue based upon evidence of actual fraudulent charges against some of the plaintiffs, the reasonable potential for future fraud against all the plaintiffs, and their expenses for credit monitoring services.[229] The Seventh Circuit reversed a district court decision that had concluded that the *Clapper* decision had "foreclose[d] any use whatsoever of future injuries to support Article III standing" in identity theft cases and instead applied a "substantial risk" standard that the *Clapper* decision had acknowledged was sometimes applicable.[230] The *Remijas* court distinguished the *Clapper* decision on the grounds that the Supreme Court's decision involved a mere suspicion that the plaintiff's communications had been monitored by the government, but that its case involved a substantial risk of harm to the plaintiffs because hackers had deliberately stolen sensitive information about the plaintiffs and 9200 customers had already suffered actual fraudulent uses of their credit cards or bank accounts.[231] The Seventh Cir-

225 *Moyer*, 2014 WL 3511500, at *6 (quoting *Clapper*, 133 S. Ct. at 1153).

226 *Id.*

227 *Id.*

228 *Id.*

229 *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693–96 (7th Cir. 2015); *see also* Fram et al., *supra* note 10 (discussing *Remijas*).

230 *Remijas*, 794 F.3d at 693; *see also* Fram et al., *supra* note 10.

231 *Remijas*, 794 F.3d at 693; *see also* Biglow, *supra* note 19, at 955–57, 967–69, 972–73, 975 (explaining that the Seventh Circuit's decision in *Remijas* found Article III standing

cuit concluded that the harms were fairly traceable to the defendant's data breach despite the possibility that some of the information might have been stolen from third parties, because standing causation requires only plausible evidence that a defendant's actions harmed the plaintiffs, and the defendant would have an opportunity at trial to demonstrate that other data breaches actually caused the harm to the plaintiffs.[232] Additionally, the court concluded that the harms were redressable by a favorable decision of the court, even though the defendant had reimbursed the plaintiffs for all of their current direct losses, where the plaintiffs alleged incidental costs from time spent correcting financial information and periods of interrupted access to credit cards and bank accounts, where there was "an objectively reasonable likelihood" of an enhanced risk of future identity theft based upon evidence that some plaintiffs had already suffered fraudulent activity, and where the defendant had implicitly acknowledged the risks of future harm by offering one year of credit monitoring.[233] Unlike Judge Bucklo, the Seventh Circuit did not discuss whether its decision in *Pisciotta* was still good law, but the court declined to address the plaintiffs' suggestion that it apply decisions "involv[ing] products liability claims against defective or dangerous products" to the data breach field because it found standing based on a substantial risk of harm from the data breach and actual evidence of fraudulent activity.[234]

4. The Ninth Circuit's Decision in *Robins v. Spokeo, Inc.*

In *Robins v. Spokeo, Inc.*,[235] the Ninth Circuit held that a defendant's alleged willful violation of the plaintiff's consumer rights under the FCRA was a violation of a statutory right sufficient to satisfy the injury-in-fact requirement for Article III standing, even if the consumer failed to allege any actual damages.[236] The *Robins* decision explicitly agreed with the Sixth Circuit's *Beaudry* decision and similar pre-*Clapper* decisions in the Ninth Circuit.[237] While it did not even cite the *Clapper* decision, the Ninth Circuit's decision in *Robins* is significant because it treated the concept of statutory standing as still valid and cited the Supreme Court's 1975 decision in *Warth v. Seldin*[238] for the principle that a statute may create legal rights that effectively establish an actual or threatened injury for Article III standing.[239] As will be discussed below, a majority of a three-judge panel in the Eighth Cir-

where 9200 persons had already been harmed by a data breach and remaining plaintiffs were therefore at a significantly increased risk of harm); Fram et al., *supra* note 10.

232 *Remijas*, 794 F.3d at 696.

233 *Id.* at 693–94, 696–97 (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)); *see also* Fram et al., *supra* note 10.

234 *Remijas*, 794 F.3d at 695.

235 742 F.3d 409 (9th Cir. 2014).

236 *Id.* at 412–14.

237 *Id.*

238 422 U.S. 490, 500 (1975).

239 *Robins*, 742 F.3d at 412.

cuit subsequently agreed with the *Robins* decision and relied upon the statutory standing principles in *Warth*, but a dissenting judge argued that the statutory standing approach in *Warth* had been effectively discredited by *Clapper* and other Supreme Court opinions requiring stronger evidence of harm to prove standing injuries.[240]

Thomas Robins sued the defendant, Spokeo, Inc., for willful violations of the FCRA related to information about the plaintiff contained on the defendant's website.[241] Spokeo's website offers users "information about other individuals, including contact data, marital status, age, occupation, economic health, and wealth level."[242] "Although he asserted that Spokeo's website contained false information about" his education and wealth level, Robins's allegations of actual harm from that allegedly false information were "sparse."[243] After initially concluding that Robins had established a sufficient injury for standing, the district court changed its view in response to Spokeo's motion for reconsideration and dismissed his case for lack of Article III standing because "Robins failed to plead an injury in fact and that any injuries pled were not traceable to Spokeo's alleged violations."[244]

On appeal, the Ninth Circuit reversed the district court's decision and held that Robins had proven a statutory standing injury pursuant to the FCRA.[245] The *Robins* decision reasoned that the plaintiff did not have to allege actual harm from the defendant's action because he alleged that Spokeo had willfully violated the statute and Congress in the FCRA sought to punish willful violations of the statute even if they do not cause an actual injury.[246] Acknowledging that Article III of the Constitution limits Congress's authority to confer statutory standing, the Ninth Circuit relied upon the reasoning in the *Beaudry* decision for the principle that statutory standing is appropriate where the plaintiff asserts that his individual statutory rights have been violated by a defendant.[247] The *Robins* decision concluded that its plaintiff met the standing test in *Beaudry*.[248] Applying the two-part test in *Beaudry* to Robins's allegations, the Ninth Circuit reasoned:

> First, he alleges that Spokeo violated *his* statutory rights, not just the statutory rights of other people, so he is "among the injured." Second, the interests protected by the statutory rights at issue are sufficiently concrete and particularized that Congress can elevate them. . . . Robins's personal interests in the handling of his credit information are individualized rather than collective.[249]

240 *See infra* subsection III.D.5.
241 *Robins*, 742 F.3d at 410–11.
242 *Id.* at 410.
243 *Id.*
244 *Id.* at 411.
245 *Id.* at 412–14.
246 *Id.* at 412.
247 *Id.* at 413.
248 *Id.*
249 *Id.*

While standing also requires a plaintiff to prove causation and redressability in addition to an injury in fact, the Ninth Circuit reasoned that causation and redressability can usually be inferred once a plaintiff proves an injury in violation of a statutory right.[250] The *Robins* decision explained:

> When the injury in fact is the violation of a statutory right that we inferred from the existence of a private cause of action, causation and redressability will usually be satisfied. First, there is little doubt that a defendant's alleged violation of a statutory provision "caused" the violation of a right created by that provision. Second, statutes like the FCRA frequently provide for monetary damages, which redress the violation of statutory rights.[251]

Accordingly, the Ninth Circuit concluded that Robins had satisfied all three parts of the Article III standing test.[252]

In 2015, the Supreme Court granted certiorari in *Spokeo, Inc. v. Robins*.[253] The issue in the case was whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute.[254] The Seventh Circuit in *Remijas* argued that the allegations of identity theft in its case "go far beyond the complaint about a website's publication of inaccurate information, in violation of the Fair Credit Reporting Act, that is before the Supreme Court in *Spokeo, Inc. v. Robins*";[255] thus, the Seventh Circuit appeared to be saying that its decision should stand even if the Supreme Court reversed the Ninth Circuit's decision.

In 2016, the U.S. Supreme Court reversed the Ninth Circuit's decision in *Spokeo, Inc. v. Robins*, a 6-2 decision authored by Justice Alito, holding that a plaintiff alleging a statutory injury in violation of a federal statute must allege not only an individualized injury, but also a concrete injury to satisfy the U.S. Constitution's Article III standing requirement for an injury in fact.[256] The Court remanded the case back to the Ninth Circuit because the court of appeals found only that Robins had an individualized injury and failed to address whether he had a concrete injury.[257] In her dissenting opinion, Justice Ginsburg, who was joined by Justice Sotomayor, maintained that Robins's particularized allegations that petitioner Spokeo, Inc., had misreported information about his employment and financial status met the concrete injury requirement because his complaint alleged that the misinformation on the

250 *Id.* at 414.

251 *Id.*

252 *Id.*

253 135 S. Ct. 1892 (2015).

254 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016); *see also* Spokeo, Inc. v. Robins, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/ (last visited Nov. 16, 2016) (providing the history of the case before the Supreme Court).

255 *Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 692 (7th Cir. 2015).

256 *Spokeo*, 136 S. Ct. at 1545, 1548, 1550 (2016).

257 *Id.* at 1550.

Spokeo site harmed his employment prospects, and, accordingly, his allegations were sufficient for standing.[258]

The majority opinion did not define what constitutes a concrete injury other than to exclude clearly harmless errors such as an "incorrect zip code."[259] The Court did state that a plaintiff enforcing a statutory right "need not allege any *additional* harm beyond the one Congress has identified."[260] The Court's rejection of an additional harm standard likely means that any plaintiff seeking information pursuant to the Freedom of Information Act (FOIA)[261] may have standing based solely upon his statutory right to information without alleging that he will suffer additional harms if he does not obtain that information.[262]

The *Spokeo* decision did not clarify the split in the lower courts about how much financial harm a plaintiff must allege to have standing in data breach or identity theft cases.[263] Citing its *Clapper* decision, the Court in *Spokeo* acknowledged that the "risk of real harm" can satisfy the concreteness requirement, and, as an example, observed that tort victims may recover "even if their harms may be difficult to prove or measure."[264] The Supreme Court's reversal of the Ninth Circuit's *Spokeo* decision might lead that Circuit to reassess whether a data breach that merely results in an increased risk of identity theft is a sufficiently concrete injury for Article III standing, but the Supreme Court's definition of concrete injury in its *Spokeo* decision is sufficiently broad that the Ninth Circuit does not need to change its approach in data breach cases.[265] "Lower court judges who favor standing in data breach cases" that do not involve actual financial losses might still conclude that the increased risk of identity theft resulting from such breaches is sufficient to "constitute both a concrete and a particularized injury."[266] The *Spokeo* decision did not directly address and leaves open the question of whether a data breach without any financial losses constitutes a concrete injury for Article III standing.

258 *Id.* at 1554–56 (Ginsburg, J., dissenting).

259 *Id.* at 1550.

260 *Id.* at 1549.

261 5 U.S.C. § 552 (2012).

262 Bradford C. Mank, *The Supreme Court's Decision and Remand in* Spokeo, Inc. v. Robins *Postpones the Difficult Standing Issues in Statutory Standing and Identity Theft Cases*, CASETEXT (May 16, 2016), https://casetext.com/posts/the-supreme-courts-decision-and-remand-in-spokeo-inc-v-robins-postpones-the-difficult-standing-issues-in-statutory-standing-and-identity-theft-cases.

263 *Id.*

264 *Spokeo*, 136 S. Ct. at 1549.

265 Mank, *supra* note 262.

266 *Id.*

5. The Eighth Circuit's Divided Decision in *Hammer v. Sam's East, Inc.*

In *Hammer v. Sam's East, Inc.*,[267] a divided three-judge panel of the Eighth Circuit agreed with the Ninth Circuit's *Robins* decision and held that a plaintiff may meet Article III standing requirements by alleging a willful violation of his individual statutory rights under a provision of the Fair and Accurate Credit Transactions Act (FACTA)[268] and seeking statutory damages under the FCRA's liability provision,[269] without a showing of actual damages from a defendant's allegedly willful violation of his rights under FACTA.[270] In his dissenting opinion, Chief Judge Riley argued that the majority's "expansive reading of a single line" in the Supreme Court's 1975 *Warth* decision was inconsistent with *Clapper* and several other post-1975 standing decisions.[271] The disagreement between the majority and Chief Judge Riley is at least partly due to the Court's unclear standing jurisprudence.[272]

a. *Hammer*'s Majority Opinion

In *Hammer*, two plaintiffs brought a putative class action on behalf of themselves and others similarly situated,

> alleg[ing] that Wal-Mart Stores, Inc., Sam's East, Inc., and Sam's West, Inc. (collectively "Sam's Club") willfully violated a provision of [FACTA], which prohibits a person accepting credit or debit cards for a consumer transaction from "print[ing] more than the last five digits of the card number . . . upon any receipt provided to the cardholder."[273]

Despite its conclusion that Sam's Club violated FACTA, the district court granted Sam's Club's motion for summary judgment dismissal on the ground that the violation was not willful because Sam's Club had printed only the last four digits of the credit card number on the receipt.[274] The district court and then the Eighth Circuit both concluded that Sam's Club's practice of printing the last ten digits of the member's identification number on his receipt, and using the full twelve digits for that identification as the member's credit card number if the member used a Sam's Club Private Label Credit Card, was a violation of FACTA, but not a willful violation of the statute because the statute was sufficiently ambiguous about whether the five-digit rule applied to membership numbers such that Sam Club's interpreta-

267 754 F.3d 492 (8th Cir. 2014).

268 15 U.S.C. § 1681c(g)(1) (2012).

269 *Id.* § 1681n(a)–(n)(a)(1)(A) ("the FCRA liability provision") ("Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of . . . any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000 . . . .").

270 *Hammer*, 754 F.3d at 498–501.

271 *Id.* at 504–08 (Riley, C.J., dissenting).

272 *See infra* subsection III.D.5.b.

273 *Hammer*, 754 F.3d at 495 (third and fourth alterations in original) (footnote omitted) (citation omitted) (quoting 15 U.S.C. § 1681c(g)(1)).

274 *Id.* at 495–97, 501.

tion was not objectively unreasonable.[275] The Eighth Circuit affirmed the district court's decision on the merits, but first concluded that the plaintiffs had Article III standing to sue.[276]

Like the Ninth Circuit in *Robins*,[277] the Eighth Circuit in *Hammer* relied upon *Warth* for the principle that "[t]he actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[278] Judge Bright's majority opinion broadly interpreted the statutory standing principle in *Warth*, stating: "Notably, this language is without limitation: the actual-injury requirement may be satisfied *solely* by the invasion of a legal right that Congress *created*."[279] Like Judge Sutton in the *Beaudry* decision,[280] the Eighth Circuit in *Hammer* cited the Supreme Court's 1982 decision in *Havens Realty Corp.* as precedent for the proposition that a statutory violation may constitute an Article III standing injury in the absence of an actual injury to an individual.[281] Responding to Judge Riley's dissenting opinion argument that *Warth* had been effectively narrowed or overruled by subsequent Supreme Court precedent, Judge Bright's majority opinion responded:

> [I]t bears repeating that to our knowledge, every federal circuit court of appeals to have addressed whether a plaintiff is permitted to recover statutory damages under the FCRA liability provision in the absence of actual damages has answered in the affirmative. Moreover, not one of these courts has concluded that the FCRA liability provision violates constitutional standing principles. Federal jurisprudence supports our holding with respect to Article III standing.[282]

Because Congress in the FCRA gave consumers a legal right to a receipt at the point of sale showing no more than five digits of a credit or debit card number, the Eighth Circuit concluded that Sam's Club's printing of more than five numbers on the receipt constituted an actual standing injury in violation of the statute, and, therefore, that the plaintiffs had Article III standing to sue.[283] Judge Bright acknowledged that standing precedent

---

275 *Id.* at 501–03. In his dissenting opinion, Chief Judge Riley argued that the statute clearly applied to membership numbers, that several Sam's Club employees had warned that its practice of printing more than five digits of the membership number violated the statute, and that a reasonable jury could decide that Sam's Club had acted in reckless disregard of its statutory duty. *Id.* at 510–13 (Riley, C.J., dissenting).

276 *Id.* at 497–501 (majority opinion).

277 *See supra* subsection III.D.4.

278 *Hammer*, 754 F.3d at 498 (alteration in original) (internal quotation marks omitted) (citation omitted) (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)).

279 *Id.*

280 *See supra* subsection III.A.2.

281 *Hammer*, 754 F.3d at 498 n.3 ("[A]n individual who receives false information in violation of section 804(d) of the Fair Housing Act has standing to bring a claim regardless of whether the violation results in actual injury to the individual." (citing Havens Realty Corp. v. Coleman, 455 U.S. 363, 373–74 (1982))).

282 *Id.* at 501 n.4.

283 *Id.* at 498–99.

required a personal injury for Article III standing, but he observed that the plaintiffs met this requirement because each alleged that his personal receipts contained excessive numbers in violation of the five-number rule in the statute.[284] Additionally, the Eighth Circuit concluded that the liability provision in the statute does not authorize suits by the public at large, but requires a plaintiff to demonstrate an individual injury to sue, in accordance with Article III standing.[285] Accordingly, the *Hammer* decision held, "Because appellants allege that they have suffered an actual, individualized invasion of a statutory right, we conclude that they have satisfied the injury-in-fact requirement of Article III standing."[286]

Next, the Eighth Circuit considered whether the plaintiffs' alleged injury was redressable by a favorable court decision, and particularly whether the plaintiffs were entitled to statutory damages in the absence of an actual injury.[287] Because the FCRA liability provision alternatively and disjunctively provides that a plaintiff may recover "any actual damages . . . or damages of not less than $100 and not more than $1,000,"[288] the *Hammer* decision concluded that a plaintiff may recover statutory damages of between $100 and $1000, even in the absence of any actual damages.[289] Furthermore, Judge Bright reasoned that allowing a plaintiff to recover statutory damages under the FCRA even in the absence of an actual injury was "consistent with the purpose of FACTA's receipt requirement" in preventing identity theft by forbidding the printing of more than the last five digits of a card number on a receipt because Congress was aware that it would be difficult in many cases of such violations to prove actual damages.[290] Additionally, the Eighth Circuit's interpretation that the FCRA allowed statutory damages in the absence of proof of actual damages was supported by the Sixth Circuit's *Beaudry* decision and similar decisions in the Seventh and Ninth Circuits.[291] In particular, the Ninth Circuit's decision in *Robins* held that a plaintiff alleging a violation of his personal statutory rights under the FCRA met Article III standing requirements and was entitled to statutory damages without showing any actual damages.[292] Accordingly, the Eighth Circuit held that the plaintiffs could recover

284 *Id.* at 499.

285 *Id.*

286 *Id.*

287 *Id.* at 499–500.

288 *Id.* at 499 (quoting 15 U.S.C. § 1681n(a)(1)(A) (2012)).

289 *Id.* at 500.

290 *Id.*

291 *Id.* (first citing Bateman v. Am. Multi-Cinema, Inc., 623 F.3d 708, 719 (9th Cir. 2010) ("Congress expressly created a statutory damages scheme that intended to compensate individuals for actual or potential damages resulting from FACTA violations, without requiring individuals to prove actual harm."); then citing Beaudry v. TeleCheck Servs., Inc., 579 F.3d 702, 705 (6th Cir. 2009) (holding that "'actual damages' represent an alternative form of relief" under 15 U.S.C. § 1681n and that "the statute permits a recovery when there are no identifiable or measurable actual damages"); and then citing Murray v. GMAC Mortg. Corp., 434 F.3d 948, 953 (7th Cir. 2006)).

292 *Id.* (citing Robins v. Spokeo, Inc., 742 F.3d 409, 413–14 (9th Cir. 2014)).

statutory damages in "the absence of a claim for actual damages," and that they met Article III standing requirements.[293]

b. Chief Judge Riley's Dissenting Opinion

In his dissenting opinion, Chief Judge Riley argued that the plaintiffs did not have Article III standing because they presented no allegations or evidence that the receipts containing their credit card information were at risk of theft by identity thieves.[294] While acknowledging that Sam's Club had committed a violation of FACTA's receipt requirement by showing more than the consumer's last five credit or debit card numbers, he contended that "this trivial statutory violation" did not constitute an injury in fact sufficient for Article III standing because no harm resulted to the plaintiffs from the violation.[295] Chief Judge Riley cited a legal dictionary and two federal courts of appeals decisions for the proposition that American civil law had historically required a plaintiff to prove he suffered an actual harm to recover monetary compensation in a suit, and then he reasoned the Supreme Court's injury-in-fact requirement for standing "incorporates this traditional principle."[296]

Chief Judge Riley criticized the majority opinion for relying upon "an extraordinarily broad reading of the Supreme Court's 1975 dictum in *Warth* that '[t]he actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'"[297] He contended that the majority's view that a plaintiff may have standing for a statutory violation without an actual injury "[i]gnor[ed] the last thirty-nine years of Article III standing jurisprudence" since the *Warth* decision and that the "Supreme Court has never actually *held* an unharmed plaintiff had standing by virtue of a bare statutory violation."[298] Since the *Warth* decision in 1975, Chief Judge Riley argued that the Court has limited Article III standing by "strongly suggest[ing] that to have a *case* under Article III, a plaintiff must have suffered not only the violation of a legal right (the 'injury' of 'injury in fact'), but also a factual harm (the 'in fact')."[299] As I will

293 *Id.* at 500.

294 *Id.* at 504 (Riley, C.J., dissenting).

295 *Id.*

296 *Id.* (citing *Injuria Absque Damno*, BLACK'S LAW DICTIONARY (9th ed. 2009) (defining *injuria absque damno*)). "It is a longstanding principle in civil law that there can be no monetary recovery unless the plaintiff has suffered harm." Mira v. Nuclear Measurements Corp., 107 F.3d 466, 473 (7th Cir. 1997); *see also, e.g.*, Pierce v. Ramsey Winch Co., 753 F.2d 416, 435 (5th Cir. 1985) ("[I]njury without damage creates no right to compensation.").

297 *Hammer*, 754 F.3d at 505 (Riley, C.J., dissenting) (alteration in original) (internal quotation marks omitted) (citation omitted) (quoting *id.* at 498 (majority opinion)).

298 *Id.* (footnote omitted).

299 *Id.* at 505–06 (first citing Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1386 (2014) ("The plaintiff must have suffered or be imminently threatened with a concrete and particularized 'injury in fact.'"); then quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 155 (2010) ("Such *harms* . . . are sufficiently concrete to satisfy the injury-in-fact prong of the constitutional standing analysis." (emphasis added by

argue below, even if Chief Judge Riley's interpretation of precedent is accurate, the Supreme Court has created confusion for the lower federal courts by "strongly suggest[ing]" an actual injury requirement for standing rather than providing a clear holding that binds lower court judges.[300]

In particular, Chief Judge Riley contended that the majority's broad reading of the *Warth* decision was inconsistent with the Supreme Court's "narrow" reading of that case in its 1992 decision *Lujan v. Defenders of Wildlife*.[301] He interpreted *Lujan*'s statement that Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law" to mean that Congress may only create a statutory remedy for a de facto harm, or in other words, an actual harm.[302] Chief Judge Riley maintained that "[w]hether Congress can create justiciable injuries where there is no real harm presents an extremely difficult constitutional question" and that "[i]t is a question the Supreme Court has never answered."[303] He questioned whether the majority's approach of allowing statutory violations to constitute a standing injury in the absence of an actual injury was inconsistent with the "Supreme Court's carefully crafted injury *in fact* jurisprudence."[304] Chief Judge Riley argued that the majority should have avoided the difficult issue of whether a standing injury may ever be recognized without an actual injury by interpreting the statute to require a plaintiff to demonstrate some amount of actual damages.[305]

c. In *Braitberg v. Charter Communications, Inc.*, the Eighth Circuit Rejects the Absolutist Approach to Statutory Standing in *Hammer*

In its 2016 decision *Braitberg v. Charter Communications, Inc.*, the Eighth Circuit interpreted the *Spokeo* decision as rejecting the absolutist approach to statutory standing in *Hammer*.[306] In the United States District Court for the Eastern District of Missouri–St. Louis, plaintiff Alex Braitberg sued defendant Charter Communications, Inc., alleging that Charter retained his personally identifiable information in violation of a section of the Cable Communications Policy Act.[307] The plaintiff relied upon the Eighth Circuit's *Hammer*

Chief Judge Riley)); then quoting Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 771 (2000) (defining "injury in fact" as "a *harm* that is both 'concrete' and 'actual or imminent, not conjectural or hypothetical'" (emphasis added by Chief Judge Riley)); and then quoting Fed. Election Comm'n v. Akins, 524 U.S. 11, 24 (1998) ("[W]here a *harm* is concrete, though widely shared, the Court has found 'injury in fact.'" (emphasis added by Chief Judge Riley))).

300 *See id.* at 505; *infra* subsection III.D.5.b.

301 *Hammer*, 754 F.3d at 506 (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)).

302 *Id.* (quoting *Lujan*, 504 U.S. at 578).

303 *Id.*

304 *Id.* at 507–08.

305 *Id.* at 508–10.

306 836 F.3d 925, 930 (8th Cir. 2016).

307 *Id.* at 926 (citing 47 U.S.C. § 551(e) (2012)).

decision for the proposition that a violation of a statutory right creates an injury in fact that is sufficient in itself to establish standing under Article III.[308] Accordingly, Braitberg argued that there is no requirement for him to allege or demonstrate an "actual injury" arising from Charter's retention of his personal information.[309] However, the district court dismissed the case for lack of Article III standing and the plaintiff appealed to the Eighth Circuit.[310]

The Eighth Circuit heard oral argument in *Braitberg* and then held the case pending a decision by the Supreme Court in *Spokeo*.[311] The Eighth Circuit concluded that Braitberg would have had standing under *Hammer*'s absolutist position that any procedural violation of a federal statute is sufficient for Article III standing.[312] However, the Eighth Circuit determined that the Supreme Court's *Spokeo* decision "rejected this absolute view [of statutory standing] and superseded [its] precedent in *Hammer*."[313] In *Braitberg*, the Eighth Circuit interpreted the *Spokeo* decision as requiring a plaintiff to demonstrate some type of concrete injury even for statutory injuries, although acknowledging that Congress may recognize intangible statutory injuries.[314] Congress may give plaintiffs the right to sue if the government fails to provide them with certain information that Congress has decided to make public.[315] However, the Eighth Circuit read the *Spokeo* decision as barring a mere procedural violation such as an incorrect zip code from establishing statutory standing.[316] The Eighth Circuit held that Braitberg's allegation of a bare procedural violation failed to meet the *Spokeo* decision's approach to statutory standing, and that he failed to establish any statutory injury.[317] The Eighth Circuit's rejection of statutory standing for bare procedural injuries in *Braitberg* does not resolve identity theft claims such as the Seventh Circuit's *Remijas* decision where there is a heightened risk of economic injury.[318]

Conclusion

Because of the split in the lower courts over whether people whose personal data has been stolen by computer hackers have Article III standing to

308 *Id.* at 930.
309 *Id.*
310 *Id.* at 927.
311 *Id.*
312 *Id.* at 930 (citing Hammer v. Sam's East, Inc., 754 F.3d 492, 498–99 (8th Cir. 2014)).
313 *Id.*
314 *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
315 *Id.* (citing *Spokeo*, 136 S. Ct. at 1549–50); *see* Bradford C. Mank, *The Supreme Court Acknowledges Congress' Authority to Confer Informational Standing in* Spokeo, Inc. v. Robins, 94 Wash. U. L. Rev. (forthcoming 2017), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833032.
316 *Braitberg*, 836 F.3d at 930 (citing *Spokeo*, 136 S. Ct. at 1550).
317 *Id.* at 930–31.
318 *See supra* Section III.D.

sue retailers or employers who failed to protect the data of consumers or employees,[319] the Supreme Court needs to address this important issue. Unfortunately, the Court's standing jurisprudence is complicated and sometimes contradictory.[320] For example, the *Clapper* decision used a strict "certainly impending" standing test, but also acknowledged that the Court had in some cases applied a less strict "substantial risk" standing standard.[321] The Court recently adopted a more lenient approach to standing in *Susan B. Anthony*,[322] and some lower court decisions granting standing in data breach cases have followed that decision or invoked the *Clapper* decision's alternative "substantial risk" standing standard.[323] In *Spokeo v. Robins*, the Supreme Court did not resolve the question of whether and under what circumstances Congress may grant Article III standing through a statute, other than to reject an additional harm requirement.[324] Thus, *Spokeo* left open the question of whether a data breach that merely increases a plaintiff's risk of identity theft is a sufficiently concrete risk to justify Article III standing.[325]

While it is difficult to predict how the Court will decide Article III standing issues in data breach cases, a recent Fourth Amendment decision holding that police officers may not search an arrested criminal suspect's cell phone without first obtaining a search warrant demonstrates that the Supreme Court is concerned with protecting the digital data of Americans.[326] In *Riley v. California*,[327] police officers, in two separate cases that were later consolidated into one appeal before the Court, had seized a cell phone from each arrested suspect, and then used digital information on the cell phone as evidence leading to a criminal conviction.[328] While prior decisions had allowed police to seize physical objects on the person of arrested subjects without a search warrant to protect the safety of police and to preserve evidence,[329] Chief Justice Roberts in a unanimous decision[330] held that police may not seize the potentially "vast quantities of personal information" stored on cell phones without first obtaining a search warrant.[331] First, he reasoned that

319 *See supra* Part III.
320 *See supra* Parts I, II.
321 *See supra* Part II.
322 *See supra* Part II.
323 *See supra* Section III.D.
324 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549–50 (2016).
325 Mank, *supra* note 262.
326 Riley v. California, 134 S. Ct. 2473 (2014).
327 *Id.*
328 *Id.* at 2480–82.
329 *Id.* at 2482–85.
330 Justice Alito wrote an opinion concurring in part and concurring in the judgment. *Id.* at 2495–98 (Alito, J., concurring in part and concurring in the judgment).
331 *Id.* at 2485–95 (opinion of the Court).

the "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[332]

The Court next addressed the balance between the government's interests in searching arrested persons and the privacy concerns of the arrestee.[333] The *Riley* decision concluded that the potentially vast amounts of information stored on modern cell phones raised far more important privacy concerns than prior cases allowing police to seize physical objects from an arrestee without a warrant, and that, accordingly, police must obtain a warrant to seize the digital data on a cell phone.[334] After observing that the digital data associated with a cell phone is sometimes actually stored in a "cloud computer" connected to the phone through the internet, the Court concluded that both data actually on the phone itself and data stored remotely is equally protected by the privacy concerns of the Fourth Amendment.[335]

In an opinion concurring in part and concurring in the judgment, Justice Alito agreed with the majority's holding that police must obtain a warrant before seizing the digital data stored on an arrestee's cell phone.[336] Because "[m]any cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form," he acknowledged the need "for a new balancing of law enforcement and privacy interests."[337] However, he suggested that Congress or state legislatures should enact statutes that balance the privacy of cell phone users against law enforcement concerns, rather than rely on the efforts of federal courts to do such balancing through the Fourth Amendment.[338]

Justice Alito's approach of recommending legislative rather than judicial solutions for cell phone users would also be helpful in the context of establishing liability rules for data breaches. There is no comprehensive federal statute addressing data breaches.[339] The FCRA and other federal statutes do not provide clear rules for liability in data breach cases, which explains in part the division in the lower courts addressing data breach issues.[340] Unfortunately, disagreements between Republicans and Democrats in Congress have blocked proposed federal legislation addressing data breach issues, and some recent proposals in Congress would arguably provide weaker remedies than some plaintiffs have won in suits involving a variety of common law or

332 *Id.* at 2485. Next, the Court addressed how police officers might secure a phone to prevent another person from wiping out or encrypting the digital data from a remote location. *Id.* at 2486–88.

333 *Id.* at 2488–91.

334 *Id.* at 2494–95.

335 *Id.* at 2491.

336 *Id.* at 2495–98 (Alito, J., concurring in part and concurring in the judgment).

337 *Id.* at 2496–97.

338 *Id.* at 2497–98.

339 Peters, *supra* note 6, at 1177–83 (discussing several federal and state statutes relevant to victims of data breaches).

340 *See supra* Part III.

indirect statutory remedies.[341] In 2014, Congress passed legislation that should improve data security in federal agencies, but these bills have no application to the private sector.[342]

There are several ways new federal data breach legislation could provide better remedies and lessen the risk of such breaches, and also balance the needs of consumers for privacy protection without overly burdening companies that cannot prevent all possible hacking of data in the internet age, but enacting legislation in Congress remains a challenge.[343] For example, a legislature might limit a plaintiff's recovery to the cost of credit monitoring services and any actual expenses incurred by a plaintiff as a result of a data breach.[344] Some states have enacted or considered legislation that limits the amount of time retailers can retain payment card data to forty-eight hours and allows financial companies to sue merchant companies that fail to comply.[345] This type of legislation should reduce the risk of future data breaches, although no proposal can assure complete security.[346]

If comprehensive legislative solutions are unlikely in the near future, federal courts should at least consider recognizing standing for plaintiffs in data breach cases where there is a significant potential for misuse of stolen data because such plaintiffs face significant harms from disclosure of their data even if they cannot prove that someone has already misused that data. The *Riley* decision involves Fourth Amendment warrant issues that are not relevant to private data breach suits.[347] Yet in both cell phone seizure cases and data breach suits, there is the common denominator that vast amounts of personal data are often at stake in a way that would have not been as true in a pre-digital age where an individual's data might have been scattered in dozens of file cabinets filled with paper.[348] The *Riley* decision could indirectly undermine the traditional view that consumers have little or no expectation of privacy in information that they voluntarily transfer to a second

341 Peters, *supra* note 6, at 1194–96 (discussing and criticizing the proposed Data Security & Breach Notification Act of 2013, S. 1193, 113th Cong. (2013)).

342 Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CAL. 229, 238–39 (2015) (listing five 2014 federal statutes addressing only data security for the federal government).

343 Peters, *supra* note 6, at 1194–1202 (proposing several legislative solutions involving private rights of action, insurance, and government regulation "to minimize the occurrence of data breaches and to provide consumers with a remedy when data breaches do occur," but acknowledging political barriers in Congress to enacting data breach legislation).

344 Rubow, *supra* note 3, at 1034–35 (citing Patricia Cave, Note, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. Rev. 765, 793 (2013)).

345 Kim, *supra* note 19, at 586.

346 *Id.* at 586–87.

347 *See* Riley v. California, 134 S. Ct. 2473, 2485–95 (2014) (discussing the privacy concerns of arrestees in the context of the Fourth Amendment).

348 *See id.* at 2489–95 (discussing the vast amounts of data stored in the current digital age compared to the pre-digital age).

party who then voluntarily or involuntarily conveys that information to a third party.[349] Courts should recognize privacy as a public good that deserves protection when defendants harm others by failing to protect their personal information.[350]

These new privacy concerns in a digital age should lead the Supreme Court to take a broader view of standing in at least some data breach cases than it did in the *Clapper* decision.[351] One must concede that the *Clapper* decision did not give much weight to privacy concerns, but that decision was different from private data breach cases because it involved the special context of government intelligence gathering.[352] It is possible that the Supreme Court's nine Justices might take a more liberal view of standing in data breach cases than in the *Clapper* decision because they could be personally affected by data breaches someday, just as their familiarity with the vast amounts of personal data stored on cell phones arguably affected their decision in *Riley*.[353]

If the Supreme Court does not address data breach standing, some courts will continue to interpret *Clapper* to bar all claims where a plaintiff only alleges possible future harms, but no current injury from the breach.[354] Some courts will rely on the substantial risk footnote in *Clapper* and the *Susan B. Anthony* decision to allow data breach suits based on future harms.[355] Other decisions will rely on the Seventh Circuit's *Remijas* decision to distinguish *Clapper* where some of the plaintiffs have suffered actual harms, on the grounds that in such cases other plaintiffs are at increased risk compared to cases where no one has suffered an actual theft of property.[356] The Seventh Circuit's *Remijas* decision's distinction between cases where there is only a possible risk of theft and cases where actual harm has occurred to some

349 Lamparello, *supra* note 3, at 123–24.

350 Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 387–96 (2015) (arguing that current legal doctrine fails to recognize privacy as a public good and therefore under-protects individual and group privacy interests).

351 *See generally* Andy Greenberg, *Why the Supreme Court May Finally Protect Your Privacy in the Cloud*, WIRED (June 26, 2014), http://www.wired.com/2014/06/why-the-supreme-court-may-finally-protect-your-privacy-in-the-cloud/ (arguing that the *Riley v. California* decision protecting the digital data of arrestees "could also signal a shift in how the Court sees the privacy of data in general—not just when it's stored on your physical handset, but also when it's kept somewhere far more vulnerable: in the servers of faraway Internet and phone companies," but focusing on governmental data collecting rather than private data breaches).

352 *See supra* Part II.

353 *See Riley*, 134 S. Ct. at 2489–95 (discussing the vast amounts of personal data stored on cell phones).

354 *See supra* Section III.C.

355 *See supra* Part II, Section III.D.

356 *See supra* Section III.D.

plaintiffs is probably the best way to decide whether there is a substantial risk of identity theft for plaintiffs until Congress is able to pass comprehensive legislation in this area.[357]

357 *See* Biglow, *supra* note 19, at 967–69, 972–73, 975 (arguing that courts should follow the Seventh Circuit's decision in *Remijas*, which found Article III standing where some persons had already been harmed by a data breach and remaining plaintiffs were therefore at a significantly increased risk of harm, rather than the Third Circuit's decision in *Reilly*, which denied standing in a data breach case with no apparent actual injuries); *supra* Section III.D, Conclusion.