BYU Law Review

Volume 2016 | Issue 4 Article 8

October 2016

Standing Room Only: Solving the Injury-in-Fact Problem for Data Breach Plaintiffs

Nick Beatty

Standing Room Only: Solving the Injury-in-Fact Problem for Data Breach Plaintiffs

I. INTRODUCTION

If something valuable is taken from you without your permission, does it matter who took it? According to modern data privacy law, it does. In fact, the answer to that simple question may end your case before it even begins.

Consider the examples of two people who had their valuable personal data taken from them by an unauthorized third party.[1] Person 1 enrolled in a cell phone plan with a major phone company and was required to give the phone company some of his private information, such as his credit card number, phone number, and home address. Person 2 started working for a company, and was required to give her employer her personal information, such as her name, address, Social Security number, date of birth, and bank account number.[2] Neither Person 1 nor Person 2 thought much about these transactions, assuming that the companies would take reasonable steps to protect their personal information.

Later, Person 1 discovered that his phone company had been giving "metadata"[3] about his (and many other people's) phone calls to the government.[4] The phone company had been giving out this data every day for the past five years or more.[5] The information given to the government was not inherently sensitive—it was not Person 1's financial information or the contents of his calls. The government had only collected information about the calls, such as which numbers Person 1 had called, how often he had made those calls, and how long

1. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) [hereinafter *ACLU*].

2. *See Reilly*, 664 F.3d at 40.

3. Metadata is "data that describes and gives information about other data," OXFORD ENGLISH DICTIONARY ONLINE (2015), or "[s]econdary data that organize, manage, and facilitate the use and understanding of primary data." BLACK'S LAW DICTIONARY (10th ed. 2014).

4. *See ACLU*, 785 F.3d at 801.

5. *See id*. at 796.

he had spent on each call.[6] All of this data collection occurred without Person 1's knowledge or permission.[7]

Person 2 discovered that a hacker broke into the network where her employer stored her personal data and gained access to the database where Person 2's personal information was stored.[8] Person 2 was told that the hacker may have stolen Person 2's credit card number, name, home address, bank account number, and even Social Security number.[9]

Concerned about the loss of their personal data, both Person 1 and Person 2 filed lawsuits. Person 1 chose to sue the government for taking his information,[10] while Person 2 sued her company for negligence in protecting her financial information.[11]

When Person 1 and Person 2 appeared in court, they were immediately faced with a question that may have surprised them. Both courts began with the same threshold inquiry: did you suffer an injury?[12] In other words, Person 1 was asked whether he was harmed when the government collected his phone call metadata without his permission. Likewise, Person 2 was asked whether she was harmed when a hacker gained access to her personal financial information. The answers to these questions had a much larger impact than either plaintiff may have expected.

The court, upon hearing Person 1's claim, determined that he had suffered an injury, and could therefore bring his case before the court.[13] However, the court hearing Person 2's claim determined that she had not actually suffered an injury at all, and therefore could not bring her claim.[14] Even though Person 1's compromised information was only metadata, and Person 2's compromised information included her financial information and Social Security number, Person 1 was able to receive redress from the courts, while Person 2 was barred.

6. *See id*.
7. *See id*. at 795–96.
8. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011).
9. *See id*.
10. *ACLU*, 785 F.3d at 787.
11. *Reilly*, 664 F.3d at 38.
12. *See id*. at 41–42; *ACLU*, 785 F.3d at 800.
13. *Reilly*, 664 F.3d at 40–42.
14. *See id*. at 42.

In the current legal environment, two people can have their personal data compromised in similar ways, yet have their claims treated in completely different manners. If the plaintiffs' personal information is accessed by the government, even if the information accessed is simply metadata, they are allowed to present their case in court.[15] But if their personal data is accessed by a private third party, no matter how sensitive the information may be, they may not get a chance at redress.[16]

This apparent discrepancy stems from the doctrine of "standing" contained in Article III of the United States Constitution.[17] According to the current interpretation of the standing doctrine, many consumers in private data breach actions have not suffered a sufficient injury-in-fact to qualify for standing, and are therefore unqualified to bring an action in court.[18] Because of this procedural hurdle, many data breach plaintiffs have been forced to resort to creative theories to qualify for standing—the most common of which is that the data breach will increase the likelihood of a potential future injury. In other words, plaintiffs claim that although they have not yet suffered harm, they are certain to be harmed in the imminent future.

This theory has been met with limited success,[19] and often creates as many problems as it purports to solve. By focusing on potential future injuries, rather than the unauthorized access itself, courts task themselves with predicting the future, instead of focusing on a present controversy. Unsurprisingly, this emphasis on injury has resulted in inconsistency and confusion in the judicial system.

The standing doctrine issue in the private data breach context has been discussed by many scholars, who have proposed various theories to try to make it easier for consumers to qualify under the standing doctrine. Some have recommended that the legislature enact a comprehensive regulatory scheme to govern data security.[20] Others

15. *ACLU*, 785 F.3d at 800.

16. *See, e.g., Reilly*, 664 F.3d at 42.

17. U.S. CONST. art. III, § 2; *see also* Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 398–404 (2014).

18. *See, e.g., Reilly*, 664 F.3d at 42.

19. *See infra* Section III.B.

20. *See* Amanda C. Border, Note, *Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States*, 35 SUFFOLK TRANSNAT'L L. REV. 363 (2012); Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is the Time?*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 34 (2009); Exec. Office of the President, ADMINISTRATION

have suggested a relaxation of some of the requirements of the standing doctrine.[21] Still others have proposed the adoption of a new, probability-based concept of injury-in-fact.[22]

This Comment suggests that such comprehensive action is not necessarily required to address the problem of standing in private data breach cases. Instead, this Comment suggests that courts recognize a right to privacy for individual personal data. If courts recognize that individuals should have a reasonable right to data security, they can eliminate the need for courts to try to predict the future. This recognition would allow courts to focus on present controversies, rather than potential future harms.

The Comment goes on to explain how courts can more effectively apply the standing doctrine in private data breach cases by adopting the injury-in-fact standard established by the United States Supreme Court in *Clapper v. Amnesty Int'l USA*.[23] This standard has proven its workability in the recent *Am. Civil Liberties Union v. Clapper* case in the Second Circuit.[24] These two cases show that the Supreme Court has already created a standard in the data security area that effectively balances plaintiffs' right to be heard with constitutional standing doctrine limitations. The only missing piece required to apply this standard is recognition of a legal right to privacy for data held by a third party. If the law were to recognize this right, either by legislation or judicial decision, the standards in *Amnesty Int'l USA* and *ACLU* would easily establish a framework for analyzing the injury-in-fact requirement in private data breach settings.

Part II of this Comment outlines the standing doctrine's injury-in-fact requirement, and explains how the requirement has limited the

DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last visited Nov. 10, 2016).

21. Miles L. Galbraith, *Identity Crisis: Seeking A Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365 (2013) (recommending a relaxation of the requirement that a future injury be "imminent" if it is to qualify as injury in fact); Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 CARDOZO L. REV. DE NOVO 119 (2015) (same).

22. *See* Jonathan Remy Nash, *Standing's Expected Value*, 111 MICH. L. REV. 1283 (2013) (proposing that courts calculate the expected value of a future injury when analyzing to find injury-in-fact).

23. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) [hereinafter *Amnesty Int'l USA*].

24. *See ACLU*, 785 F.3d at 800–03.

ability of consumers to bring private data breach claims. Part III then demonstrates how plaintiffs have turned to more creative theories to show injury-in-fact, particularly the potential-future-injury theory. It also shows how the judiciary's focus on this theory has resulted in an unclear, inconsistent standard in private data breach cases. Lastly, Part IV demonstrates how recognizing a legal right to privacy for personal data held by a third party can resolve the injury-in-fact issues facing data breach plaintiffs and allow courts to better focus on current controversies rather than potential future harms. It concludes by showing how the standard set by the United States Supreme Court in *Amnesty Int'l USA* can be applied in private data breach cases to effectively balance consumers' rights with constitutional justiciability limitations.

II. STANDING AND THE INJURY-IN-FACT REQUIREMENT

Plaintiffs in data breach claims often find themselves arguing issues involving the United States Constitution at the very start of litigation.[25] Article III of the United States Constitution limits federal judicial power to the resolution of "Cases" and "Controversies."[26] From this language, the United States Supreme Court has established a set of rules that limit a plaintiff's ability to bring a claim.[27] These rules are often called the justiciability doctrine,

25. *See* Cease, *supra* note 17, at 398–404.

26. U.S. CONST. art. III, § 2.

27. James Leonard & Joanne C. Brant, *The Half-Open Door: Article III, the Injury-in-Fact Rule, and the Framers' Plan for Federal Courts of Limited Jurisdiction*, 54 RUTGERS L. REV. 1, 2 (2001).

which includes concepts such as ripeness,[28] mootness,[29] political questions,[30] and standing.[31]

The aspect of justiciability that arises most often in data breach claims is the standing requirement.[32] If a plaintiff cannot demonstrate that she has standing to bring a claim, a court will dismiss the case before reaching the merits.[33] To meet the standing requirement, a plaintiff must show: 1) that she has suffered an "injury-in-fact," 2) that the injury is traceable to the defendant, and 3) that the requested relief will redress the injury.[34] The first standing requirement—"injury-in-fact"—is usually the justiciability hurdle that data breach plaintiffs have the most difficulty in overcoming.[35] To sufficiently demonstrate injury-in-fact, a plaintiff must show an injury that is "concrete and particularized," or "actual or imminent," and that is not "conjectural or hypothetical."[36] In other words, a plaintiff must prove that he has a personal stake in the litigation by "show[ing] that he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant."[37]

28. Ripeness "seeks to separate matters that are premature for review." ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 92 (3d. ed. 2009). There is some overlap between ripeness and the injury requirement in standing doctrine, but ripeness is perhaps best understood as a question of when courts can grant pre-enforcement review of a statute or regulation. *Id.*; *see also* Gene R. Nichol, Jr., *Ripeness and the Constitution*, 54 U. CHI. L. REV. 153, 161 (1987).

29. The mootness doctrine requires that the controversy be live at all points of the litigation, not just the outset. For example, if a criminal defendant dies during an appeal, the case becomes moot. *See* CHEMERINSKY, *supra* note 28, at 97; *see also* Steffel v. Thompson, 415 U.S. 452, 459 n.10 (1974).

30. The political question doctrine refers to the rule that some questions should be left to the political branches of government, rather than heard by the court. *See* CHEMERINSKY, *supra* note 28, at 103; *see also* Baker v. Carr, 369 U.S. 186, 210 (1962).

31. *See* CHEMERINSKY, *supra* note 28, at 45–46.

32. Timothy H. Madden, *Data Breach Class Action Litigation – A Tough Road for Plaintiffs*, 55 BOS. B.J. 27, 29 (2011).

33. *See, e.g.*, Sierra Club v. Morton, 405 U.S. 727, 741 (1972) ("As we conclude that the Court of Appeals was correct in its holding that the [plaintiff] lacked standing to maintain this action, we do not reach any other questions presented in the petition, and we intimate no view on the merits of the complaint.").

34. *See* Allen v. Wright, 468 U.S. 737, 751 (1984), *abrogated by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377 (2014).

35. *See* Galbraith, *supra* note 21, at 1376.

36. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (holding that a plaintiff in an environmental case lacked standing to challenge certain environmental regulations).

37. Gladstone, Realtors v. Vill. of Bellwood, 441 U.S. 91, 99 (1979); *see also* Leonard & Brant, *supra* note 27, at 2.

Usually, plaintiffs can easily demonstrate injury-in-fact by pointing to a physical or financial harm. In most cases where a plaintiff alleges one of these types of damage, courts do not even address the injury-in-fact requirement. The injury is so obvious to each party that the question is not disputed. The United States Supreme Court has also recognized that, even when a plaintiff does not have physical or financial harm, congressional actions can create individual legal rights that qualify a plaintiff for the injury-in-fact requirement.[38] If one of these legislatively created rights is violated, it "can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute."[39] The same principle applies to constitutionally created rights.

But even when a plaintiff does not have a legislative or constitutional right, and cannot show a physical or financial harm, she still may be able to qualify for the injury-in-fact requirement.[40] Courts have often recognized injury-in-fact in cases where, in absence of a financial harm, plaintiffs allege an abstract, intangible, or even "spiritual" injury.[41] For example, plaintiffs have qualified for standing without showing a physical or financial harm in actions for trespass, defamation, breaches of contract, and loss of recreational opportunities.[42]

38. Linda R.S. v. Richard D., 410 U.S. 614, 617 n. 3 (1973) ("Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.").

39. Warth v. Seldin, 422 U.S. 490, 514 (1975).

40. F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 281 (2008).

41. Galbraith, *supra* note 21, at 1377.

42. *See* Hulle v. Orynge, Y.B. 6 Edw. 4, fol. 7, Mich, pl. 18 (1466), reprinted in A.K.R. KIRALFY, A SOURCE BOOK OF ENGLISH LAW 128–32 (1957) (trespass); Time, Inc. v. Firestone, 424 U.S. 448, 460 (1976) (defamation); Foley v. Wells Fargo Bank, N.A., 772 F.3d 63, 77 (1st Cir. 2014) (breach of contract); Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167 (2000) (loss of recreational opportunities). In many of these cases, courts have not only held that the plaintiffs do qualify under the injury-in-fact requirement even without physical or financial harm, but have often awarded nominal damages to the plaintiffs. *See, e.g.*, 75 Am. Jur. 2d Trespass § 112 ("In the absence of proven or actual damages, plaintiffs are entitled to nominal damages in an action for trespass. The limited right to recover nominal damages in an action for trespass to real property is appropriate when needed to protect an important right, even absent any substantial loss or injury."); *see also* THEODORE SEDGWICK, A TREATISE ON THE MEASURE OF DAMAGES ch. VI, §§ 96–109, at 164–91 (Arthur G. Sedgwick & Joseph H. Beale eds., 9th ed. 1920) (listing hundreds of cases awarding nominal damages for violations of non-economic rights).

However, most courts in data breach cases have been hesitant to recognize the loss of personal data as the same kind of justiciable "intangible injury" recognized in trespass actions.[43] These courts often insist that the loss of personal data by itself is not enough to qualify as injury-in-fact.[44] Courts usually ask data breach plaintiffs to show that their data was not only stolen, but also misused in a way that resulted in additional, economic damage.[45]

This insistence upon economic damage causes problems for many data breach plaintiffs. In many cases, consumers who have had their personal information accessed bring claims against companies soon after they learn about the data breach—often before a third-party hacker uses the information to attempt identity theft or credit card fraud.[46] Thus, many data breach plaintiffs are turned away for lack of standing and are therefore unable to present the merits of their claims.

Faced with this difficulty in establishing injury-in-fact, consumers have developed increasingly creative theories to overcome the obstacle. Some courts have accepted these creative theories,[47] perhaps recognizing some injustice in requiring a consumer to wait patiently for his information to be used against him before he is allowed to bring a claim. However, many other courts have been hesitant to recognize these more creative methods of qualifying for the injury-in-fact requirement.[48]

43. Galbraith, *supra* note 21, at 1379.

44. *See, e.g.*, Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006).

45. Galbraith, *supra* note 21, at 1379. It is also possible that the "third-party doctrine" has an influence on courts in data breach cases. The third-party doctrine states that when a person voluntarily gives information to a third party, the person foregoes any privacy rights he has in that information. *See* United States v. Miller, 425 U.S. 435, 442 (1976); *see also* Katz v. United States, 389 U.S. 347, 351 (1967). Though the third-party doctrine has never been explicitly raised in a data breach case, since it was created and has been discussed almost exclusively in the context of 4th amendment searches and seizures, *see, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009) (defending the third party doctrine and analyzing cases where it has been applied), some commentators have suggested that the third-party doctrine is one of the reasons that courts are hesitant to grant standing to data breach victims. *See* Lamparello, *supra* note 21, at 120.

46. *See* Cease, *supra* note 17, at 399.

47. *See infra* Section III.B.

48. 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. 3, 27 (2014).

III. CONSUMER ATTEMPTS TO QUALIFY FOR STANDING

Consumers have asserted many different theories of injury-in-fact in their struggle to overcome the hurdle posed by the standing requirement. These theories range from a theory of injury through emotional distress to a theory of breach of implied contract.[49] But perhaps the most common theory of injury that data breach plaintiffs have come to rely on is the theory of potential-future-injury.

A. The Potential-Future-Injury Theory

The potential-future-injury theory is based on the idea that, though an event has not caused injury to the plaintiff yet, it has increased the risk of an injury occurring in the future. Possibly the most common use of this theory has been outside of data breach settings, in cases involving environmental protection, such as *Lujan v. Defenders of Wildlife*[50] and *Friends of the Earth v. Laidlaw*.[51] The Supreme Court's reasoning in these decisions has framed much of the debate in other potential-future-injury cases, including many private data breach cases.

In the frequently cited *Lujan* case, an environmental organization challenged new regulations that changed the effect of the Endangered Species Act.[52] The new regulations allowed the federal government to avoid certain statutory obligations for projects outside of the United States.[53] One plaintiff, a member of an environmental organization, claimed that the new regulations "w[ould] seriously reduce endangered . . . species habitat" in areas that she had previously visited.[54] The plaintiff claimed that she had suffered an injury-in-fact because she "intend[ed] to return to [the foreign habitats] in the future."[55] The U.S. Supreme Court was not convinced by this theory—especially after one plaintiff admitted that she did not have current plans to visit the habitat, because it was in the middle of a

49. *Id.* at 28–30, 55, 60.
50. 504 U.S. 555 (1992).
51. 528 U.S. 167 (2000).
52. *Lujan*, 504 U.S. at 558.
53. *Id.*
54. *Id.* at 563.
55. *Id.*

country embroiled in a civil war.[56] The Court held that "'some day' intentions—without any description of concrete plans, or indeed any specification of *when* the some day will be" were not sufficient to establish standing.[57]

The *Lujan* decision did not put a stop to environmental claims based on abstract theories of potential future injury-in-fact. Eight years later, in *Friends of the Earth, Inc. v. Laidlaw Environmental Servs. (TOC), Inc.*, the U.S. Supreme Court again faced a case involving environmental harm, and this time the Court came to a different conclusion.[58] In *Friends of the Earth*, an environmental organization sued Laidlaw for discharging excessive amounts of pollutants into a river.[59] The organization claimed injury-in-fact on the theory that the pollution had limited local residents' ability to use the river for recreation.[60] For example, one member of the organization stated that

> he lived a half-mile from Laidlaw's facility; that he occasionally drove over the . . . [r]iver, and that it looked and smelled polluted; and that he would like to fish, camp, swim, and picnic in and near the river between 3 and 15 miles downstream from the facility, as he did when he was a teenager, but would not do so because he was concerned that the water was polluted by Laidlaw's discharges.[61]

The Court stated that these kinds of "conditional statements" could not be equated with the "speculative 'some day' intentions" in *Lujan*,

56. *Id.* at 563–64.

57. *Id.* at 564. *But see id.* at 582 (Stevens, J., concurring) (arguing that the plaintiffs did have standing since "[a]n injury to an individual's interest in studying or enjoying a species and its natural habitat occurs when someone . . . takes action that harms the species and habitat."); *id.* at 592 (Blackmun, J., dissenting) (asserting that plaintiffs did have standing since a fact finder could conclude, based on the plaintiffs "statements of intent to return, . . . past visits to the [habitats], as well as their professional backgrounds, that it was likely that [the plaintiffs] would make a return trip to the [habitats].").

58. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167 (2000).

59. *Id.* at 176.

60. *Id.* at 181–83.

61. *Id.* at 181–82 (The other members of the organization made similar statements. One member stated that she no longer picnicked, walked, or birdwatched near the river out of concerns about pollutants. Another attested that her home had a lower value than similar homes located farther from Laidlaw's facility.); *see also id.* at 183 (Another member averred that he had canoed downriver from the facility, and would like to canoe closer, but would not because of the pollutants.).

and held that the Friends of the Earth members *did* meet the injury-in-fact requirement.[62]

These two cases laid out the principles of the potential-future-injury theory. The Supreme Court realized that recognizing *all* potential future injuries as injuries-in-fact could unduly expand the power of federal courts.[63] To address this concern, the Court limited the theory's applicability to injuries that are "actual or imminent," and not merely "hypothetical."[64] The theory was then picked up by private data breach plaintiffs in their efforts to overcome the injury-in-fact hurdle created by the standing doctrine. However, many courts have been hesitant to recognize injury-in-fact for data breach plaintiffs that rely on a potential-future-injury theory of harm.

B. The Potential-Future-Injury Theory in Private Data Breach Claims

Plaintiffs with private data breach claims usually advance the potential-future-injury theory using two arguments. First, plaintiffs contend that the unauthorized access to their personal data has increased the likelihood that they will suffer financial damage in the future, such as by identity theft or fraudulent charges on their bank accounts.[65] As a corollary to this theory, plaintiffs sometimes also argue that they have suffered current financial harm because they have spent money trying to mitigate future injuries, such as by

62. *Id*. at 184.

63. Hessick, *supra* note 40, at 297; *see also* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

64. Whitmore v. Arkansas, 495 U.S. 149, 155 (1990); *Lujan*, 504 U.S. at 560; *see also* Diamond v. Charles, 476 U.S. 54, 66 (1986) (rejecting standing based on "unadorned speculation"); City of Los Angeles v. Lyons, 461 U.S. 95, 109 (1983) (denying standing to an individual seeking to challenge police chokehold because it was only speculative that the plaintiff would be subjected to chokehold); Ashcroft v. Mattis, 431 U.S. 171, 171–72 n.2 (1977) (denying standing in a claim challenging police use of deadly force against a person attempting to escape arrest); O'Shea v. Littleton, 414 U.S. 488, 497 (1974) (denying standing to residents who sought injunctive relief against judges allegedly engaged in a pattern and practice of discriminatory practices on the ground that the threat to plaintiffs from this discrimination was only "speculation and conjecture"); Golden v. Zwickler 394 U.S. 103, 109 (1969) (denying standing for a claim based on the potential future candidacy of a former Congressman); United Pub. Workers v. Mitchell, 330 U.S. 75, 89–91 (1947) (stating that a "hypothetical threat [of enforcement] is not enough" for jurisdiction); Pub. Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1294 (D.C. Cir. 2007) (denying standing for claim of speculative future injury), modified on reh'g by 513 F.3d 234 (D.C. Cir. 2008) (per curiam).

65. Jacobus & Watson, *supra* note 48, at 28.

purchasing credit monitoring services.[66] While other plaintiffs have advanced alternative theories of harm, such as emotional damage[67] or breach of implied contract,[68] the potential-future-injury theory has been the most common.[69]

Circuit courts have come to different conclusions in the application of these two theories to private data breach cases. For example, in 2011, the Third Circuit addressed the potential-future-injury theory in *Reilly v. Ceridian Corp.*[70] In *Reilly*, a hacker infiltrated Ceridian's computer system, which held the personal and financial information of up to 27,000 employees at 1,900 companies.[71] The personal data included names, addresses, Social Security numbers, dates of birth, and bank account information.[72] Neither the plaintiffs nor Ceridian Corp. knew for certain whether the hacker actually read, copied, or used the personal data.[73] After the breach, Ceridian Corp. sent letters to notify the employees of the event, and arranged for one year of free credit monitoring and identity theft protection.[74]

Even though Ceridian Corp. voluntarily offered credit monitoring and protection, some employees filed suit against the company. To establish injury-in-fact, the employees relied on the potential-future-injury theory, claiming that they suffered an increased risk of identity theft because of the data breach.[75] The Third Circuit, however, held that the employees' "string of hypothetical injuries" did not meet the injury-in-fact requirement.[76] Specifically, the court noted that the employees could not show that the hacker actually read the

66. *Id*. at 16–17.

67. *Id*. at 46–47. The plaintiffs in both *Reilly v. Ceridian Corp*. and a similar case, *Krottner v. Starbucks Corp*., 628 F.3d 1139 (9th Cir. 2010), asserted the emotional distress theory of injury. The *Krottner* court, which had accepted the "potential future harm" theory, also accepted the emotional distress contention, while the *Reilly* court, which did not accept the "potential future harm" argument, also rejected the plaintiff's emotional distress argument. *Id*. at 1142; Reilly v. Ceridian Corp., 664 F.3d 38, 45–46 (3d. Cir. 2011).

68. Jacobus & Watson, *supra* note 48, at 37–39; *see also* Katz v. Pershing, 672 F.3d 64, 72 (1st Cir. 2012) (holding that a breach-of-contract theory could establish injury-in-fact).

69. Jacobus & Watson, *supra* note 48, at 17.

70. *Reilly*, 664 F.3d at 38.

71. *Id*. at 40.

72. *Id*.

73. *Id*.

74. *Id*.

75. *Id*.

76. *Id*. at 44.

information, or that the hacker intended to misuse the data. Because "there [was] no evidence that the intrusion was intentional or malicious," the potential future harm was not sufficiently imminent to qualify as injury-in-fact.[77]

Though the Third Circuit did not find injury-in-fact in *Reilly*, other circuits have found injury-in-fact when applying the same potential-future-injury test in a similar data breach situation. For example, in 2007, the Seventh Circuit Court of Appeals addressed the potential-future-injury theory in *Pisciotta v. Old Nat'l Bancorp*.[78] In *Pisciotta*, banking customers alleged that Old National Bancorp failed to adequately secure their personal information.[79] The plaintiffs claimed the bank suffered a security breach, and the plaintiffs' information was accessed by a third party.[80] The plaintiffs whose data had been accessed did not claim to have suffered any "*completed direct* financial loss to their accounts," or claim that they were victims of identity theft.[81] Instead, they claimed to have suffered "substantial potential economic damages," and added that they had incurred expenses to mitigate the potential-future-injury.[82] The Seventh Circuit accepted these facts as sufficient to qualify the plaintiffs for the injury-in-fact requirement.[83] In doing so, the Seventh Circuit stated the plaintiffs qualified for the injury-in-fact requirement because "[e]ven a small probability of injury is sufficient to create a case or controversy—to take a suit out of the category of the hypothetical."[84]

77. *Id*. The Third Circuit apparently envisioned a possibility that a third-party hacker could either unintentionally penetrate a company's firewall to gain access to personal employee information, or would intentionally do so, but for non-malicious reasons.

78. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

79. *Id*. at 631.

80. *Id*.

81. *Id*. at 632 (emphasis in original).

82. *Id*.

83. *Id*. at 632, 634.

84. *Id*. at 634 n.4 (citing Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir. 1993)). The Seventh Circuit also noted that in other areas of tort law such as toxic tort and medical malpractice, "a cognizable injury for standing purposes" is created even when exposure to toxic substances or defective medical devices only increase the risk of future harm. *See e.g.*, *Pisciotta*, 499 F.3d at 634 n.3 (citing Denney v. Deustche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (toxic tort); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (defective medical device); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (environmental tort); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (environmental tort)).

In 2010, the Ninth Circuit also accepted the potential-future-injury theory of injury-in-fact in *Krottner v. Starbucks Corp.*[85] In *Krottner*, a laptop containing the names, addresses, and Social Security numbers of 97,000 employees was stolen from a Starbucks store in Washington.[86] Starbucks informed the affected employees of the theft and offered a year of credit watch services so that employees could monitor for identity theft.[87] Two employees filed a lawsuit against Starbucks over the incident.[88] Both employees alleged that after receiving the letter, they spent "a substantial amount of time" monitoring their 401(k) and bank accounts to prevent identity theft.[89] One of the plaintiffs was notified by his bank that someone had tried to open a new account using his Social Security number, but that the bank closed the account; the plaintiff suffered no financial loss.[90] The Ninth Circuit court held that because there was a "credible threat of real and immediate harm stemming from the theft," the plaintiffs qualified under the injury-in-fact requirement.[91]

These cases illustrate the different results that courts can reach when faced with largely similar data breach fact patterns. In *Krottner*, the Ninth Circuit found injury-in-fact when a third party stole a laptop with a plaintiff's financial data.[92] And in *Pisciotta*, the Seventh Circuit did find injury-in-fact when a third party breached a bank's network and accessed the plaintiff's financial data.[93] Yet in *Reilly*, the Third Circuit did not find injury-in-fact when a hacker infiltrated a company's network and accessed a plaintiff's personal and financial data.[94]

85. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
86. *Id.*
87. *Id.* at 1141.
88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.* at 1143.
92. *Id.* at 1140.
93. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007).
94. Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d. Cir. 2011).

C. Difficulty and Inconsistency in Applying the Potential-Future-Injury Theory

The results in these data breach cases illustrate the difficulties and inconsistencies that invariably arise when courts apply the potential-future-injury theory. Circuits that have addressed the theory have often come to opposing results, even in situations with similar fact patterns.[95] Circuit courts have applied the test in similar factual scenarios, and have reached completely different results.

This inconsistency arises because applying the potential-future-injury test requires courts to peer into the future to determine how likely it is that a future risk will actually occur. Not only does this approach result in inconsistent results, it also arguably stretches the doctrine of standing farther than the Constitution intended.[96] Recognizing all potential future risks seems to contradict the idea that justiciable claims must be based on a "case[]" or "controvers[y]."[97] Instead of analyzing what has happened already, the theory requires courts to decide if something will happen in the future.

These inconsistent results have caused uncertainty in the law surrounding private data breach claims.[98] As noted above, some circuits seem to be more lenient when applying the potential-future-injury theory than others. As yet, courts have not established a uniform test for applying the potential-future-injury theory in data breach cases that achieves consistent results.[99] Overall, the potential-future-injury theory stretches the case or controversy concept to unrecognizable limits, asks courts to predict the future, and achieves inconsistent results—the theory is not a reliable way to govern private data breach cases in a modern, digital age.

95. *See* Galbraith, *supra* note 21, at 1369 n.22.

96. *See* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) ("Given the multiple strands of speculation and surmise from which the plaintiff's hypothesis is woven, finding standing in this case would stretch the injury requirement past its breaking point."); Patricia Cave, *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, 784 (2013) (arguing that allowing an increased risk of harm to qualify as standing in all data breach cases would "[s]tretch[] the [d]octrine to [i]ts [l]imits").

97. U.S. CONST. art. III, § 2.

98. Jacobus & Watson, *supra* note 48, at 29.

99. Cease, *supra* note 17, at 421. *But see* Jacobus & Watson, *supra* note 48, at 29 (analyzing case law to identify some common factors used by courts in resolving the injury-in-fact issue).

IV. A SIMPLE SOLUTION TO THE PRIVATE DATA BREACH PROBLEM

The standing doctrine, particularly the injury-in-fact requirement, has hindered the goals of both consumers and courts in private data breach cases. Obviously, consumers are inconvenienced when they are barred from bringing an action when a third party steals their personal data. Consumers must choose between bringing a claim before their personal data is used against them (which involves litigating a threshold constitutional issue), or waiting for their data to be misused before bringing the action.

The standing doctrine also puts courts in an uncomfortable situation. Because plaintiffs can only prove injury-in-fact through the potential-future-injury theory, courts are required to engage in guesswork to determine whether a future injury is a "credible threat of real or immediate harm"[100] or a mere "string of hypothetical injuries."[101] Courts addressing this theory must attempt to foresee the future, which is precisely the activity that the "cases and controversies" language in the Constitution is designed to prevent.

A. Proposed Methods of Addressing the Problem

Many commentators have attempted to solve the standing problem for private data breach claims. Their solutions have ranged from comprehensive data security legislation,[102] to relaxing the requirement that an injury be imminent,[103] to recognizing the "expected value" of potential future financial harm as sufficient to meet injury-in-fact.[104] These solutions could help clarify the law surrounding injury-in-fact, but none of them are an instant cure-all. Some may introduce as many problems as they solve, and all of the proposals would likely be complicated to adopt. These complications have meant that, so far, courts have been hesitant to adopt any of these solutions.

Many scholars have called for Congress to step in and regulate the area of data security, stating that "more comprehensive federal

100. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).
101. Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011).
102. Galbraith, *supra* note 21; *see* Cave, *supra* note 96, at 789.
103. *See* Lamparello, *supra* note 21.
104. *See* Nash, *supra* note 22.

legislation is necessary to protect consumers from cybersecurity threats."[105] The first proposed solution—comprehensive federal legislation—would be the most all-encompassing way to deal with the problem. Comprehensive legislation would establish individual privacy rights, and could also provide a unique standard for courts to use when addressing whether a plaintiff has standing to bring a claim. Even the executive branch has called for legislation to be enacted, first by publishing an executive report calling for Congressional action,[106] and then proposing a bill of its own that would establish comprehensive regulatory change.[107] As yet, however, no federal legislation has been enacted, leaving only a "constantly changing patchwork of state laws."[108]

While comprehensive legislation in this area of law may be the ideal solution, there is no telling when or if federal legislation will be enacted. Bills intended to regulate data security have been proposed to both houses of Congress since at least 2006.[109] Currently, there are numerous bills before the 114th session of Congress that seek to regulate data security on a large scale.[110] However, most of the bills from previous years did not make it past the committee stage, and as of yet, none of the current bills have passed a House or Senate vote.[111]

Moreover, many of the bills that have been proposed would not address the standing issue for many data breach plaintiffs even if they were enacted. Generally, the bills do not focus on recognizing an

105. Galbraith, *supra* note 21, at 1375.

106. Exec. Office of the President, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

107. Exec. Office of the President, *supra* note 20.

108. Julie A. Heitzenrater, *Data Breach Notification Legislation: Recent Developments*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 661, 663 (2009).

109. *See, e.g.*, Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2006); Data Security Act of 2007, H.R. 1685, 110th Cong. (2007).

110. *See, e.g.*, Secure Data Act of 2015, S. 135, 114th Cong. (2015); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015); Data Security Act of 2015, S. 961, 114th Cong. (2015); Data Security Act of 2015, H.R. 2205, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015); Secure and Protect Americans' Data Act, H.R. 4187, 114th Cong. (2015).

111. The furthest along at the time of writing are House Bill 2205, and House Bill 1770, which were sent to the House for consideration on December 9, 2015 and April 15, 2015 respectively.

individual right against unauthorized access to data, but instead focus on requiring companies to notify individuals if their information has been subject to unauthorized access.[112] Even if one of the notification-focused bills were enacted by Congress, it would only give individuals a claim if their data was accessed *and* the company did not notify them of the breach; it would not give an individual the right to pursue a claim based on the breach alone. A federal act of this type would not necessarily help the plight of data breach victims, since many states already have notification laws in place.[113]

The second proposed solution to solve the data breach standing problem is to retain the potential-future-injury theory, but relax the requirement that harms must be imminent to qualify as injury-in-fact.[114] Scholars that make this suggestion generally agree with the concept of the potential-future-injury theory, but argue that courts have been too strict in their insistence that a future injury must be impending.[115] Proponents of this method typically make the same arguments that were used in the opinions in *Krottner* and *Pisciotta*, reasoning that if the future-injury framework is good enough for toxic exposure, medical defect, and environmental cases, then it should also work for data breach cases.[116] While adopting this approach may better protect individual consumers' rights, it would not solve many of the problems that currently afflict the potential-future-injury theory.

Retaining the potential-future-injury framework would still require courts to predict the future by forcing them to consider a possible future occurrence instead of allowing them to focus on a present "controversy." Courts would probably still come to inconsistent results, even if the standard is relaxed.[117] Retaining the future-injury standard would not eliminate the difficulty courts have had in applying the standard—it would only move the goalposts, not change the rules of the game. Keeping the potential-future-injury standard, even in a relaxed form, would probably result in a legal environment that is just as muddied as it is today.

112. *See* Heitzenrater, *supra* note 108, at 676; *see also* H.R. 1770; S. 177.

113. Michael E. Jones, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 I/S: J.L. & POL'Y INFO. SOC'Y 555, 574 (2008).

114. Galbraith, *supra* note 21, at 1387; Lamparello, *supra* note 21, at 128.

115. Galbraith, *supra* note 21, at 1387.

116. *Id*. at 1388–96.

117. *See supra* Section III.C.

A third proposed solution is for courts to adopt an "expected value" model of analyzing future injuries.[118] Jonathan Nash, in his article, *Standing's Expected Value*, argues that courts should resolve the standing question by deciding whether a plaintiff has suffered a harm with a positive "expected value."[119] This value would be calculated by multiplying the probability of a future harm by its likely magnitude.[120] If the value of that calculation "would be sufficient to support standing were it to arise as a typical 'actual harm,'" then the plaintiff's damage would qualify as injury-in-fact.[121]

This alternative method of analyzing injury-in-fact would be a unique way to solve the future-injury issue. On first glance, it would give courts a clear, numerical way to calculate whether a potential future harm qualifies. However, this method would actually worsen the problem in other ways. The "expected value" method would still require courts to predict the future, rather than focus on present controversies. But in addition to the future-gazing that courts do now, they would also need to quantify both the magnitude of any potential harm, and its probability of occurring. Though Nash contends that courts routinely quantify similar risks when setting bail or a preliminary injunction,[122] those quantification processes differ from the proposed method for quantifying data breach claims. For example, to set bail, one of the factors courts use is a defendant's financial circumstances.[123] Having a certain, established figure to start from undoubtedly makes the process of setting bail much easier. With the "expected value" method, courts would not have the benefit of starting from a set figure, but would have to speculate to create both the magnitude of possible damages and the probability of the damages occurring. Applying such an uncertain method without any concrete starting point would probably result in the same inconsistency and uncertainty that plagues data breach victims today.[124]

118. *See* Nash, *supra* note 22, at 1306.
119. *Id*.
120. *Id*.
121. *Id*.
122. *Id*. at 1316–19.
123. 18 AM. JUR. PROOF OF FACTS 2D 149.
124. *See supra* Section III.C.

B. A Simpler Solution

Most of the solutions posited by scholars and policymakers would require either comprehensive legislation, or a completely new judicial standard. However, there is a simple, easy solution that would better apply the standing doctrine with only minimum changes to the current law. This solution is possible because a workable standard has already been established—in the specific setting of unauthorized access to personal data—by the United States Supreme Court.[125] Not only has the Supreme Court established the relevant standard, the standard has also already been applied by a Circuit Court in a similar case.[126] This ready-made standard already exists, more closely follows the standing requirement, and would be much easier to apply than the current uncertainty of the potential-future-injury theory.

1. The injury-in-fact standard in government cases

Two recent cases, *Amnesty Int'l USA*[127] and *Am. Civil Liberties Union v. Clapper*,[128] created a workable injury-in-fact standard that could easily be used by courts to analyze private data breach actions. The standard has already proven effective in preventing frivolous data breach claims, while still allowing plaintiffs who have experienced an actual loss to have their day in court.

The Supreme Court case that established the standard was *Amnesty Int'l USA*.[129] In *Amnesty Int'l USA*, the Supreme Court ruled on a constitutional challenge to a 2008 amendment to the Foreign Intelligence Surveillance Act (FISA).[130] FISA was originally enacted in 1978 to regulate government electronic surveillance for foreign intelligence.[131] In 2007, prompted by a perceived need to combat terrorism, the Executive branch of the U.S. Government asked Congress to amend the FISA to expand the government's authority to use electronic surveillance.[132] Congress obliged by enacting the

125. *See Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013).
126. *See ACLU*, 785 F.3d 787 (2d Cir. 2015).
127. *Amnesty Int'l USA*, 133 S. Ct. at 1138.
128. 785 F.3d at 787.
129. *Amnesty Int'l USA*, 133 S. Ct. at 1138.
130. *See* Foreign Intelligence Surveillance Act of 1978, § 101 50 U.S.C. § 1801 *et seq.*
131. *Amnesty Int'l USA*, 133 S. Ct. at 1143.
132. *Id.* at 1144.

FISA Amendments Act of 2008,[133] which "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA."[134]

After the amendments were enacted, Amnesty International USA, an organization of human rights activists, sued James R. Clapper, the Director of National Intelligence, claiming that the new amendment violated the constitutional protections against illegal search and seizure in the Fourth Amendment.[135] The activists sought an injunction against Clapper to prohibit him from ordering electronic surveillance under the newly amended act.[136] To address the issue of injury-in-fact, the activists claimed that because their work required them "to engage in sensitive international communications with individuals who they believe are likely targets of surveillance," they were particularly sensitive to future government surveillance.[137] Therefore, the activists claimed they had suffered injury-in-fact when the amendment was passed, since the amendment created "an objectively reasonable likelihood" that their communications would be intercepted by the government in the future.[138] The activists also argued that, in the alternative, they had suffered injury-in-fact because they had undertaken "costly and burdensome measures to protect the confidentiality of their international communications."[139]

The Supreme Court, in a 5-4 decision, disagreed with both of the activists' theories.[140] The Court stated that, even if the amendment made the possibility of future surveillance more likely, such a future possibility was too speculative to meet the injury-in-fact

133. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2008); Foreign Intelligence Surveillance Act of 1978, § 702, 50 U.S.C. § 1881(a) (2008).

134. *Amnesty Int'l USA*, 133 S. Ct. at 1143; 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS §§ 3.1, 3.7 (2d ed. 2012). The amended version of the statute allowed the government to start surveillance without demonstrating probable cause that the target was a foreign power. It also did not require the government to specify the nature and location where the surveillance would take place.

135. *Amnesty Int'l USA*, 133 S. Ct. at 1142. The Fourth Amendment protects U.S. citizens against unreasonable searches and seizures. *See generally* WAYNE R. LEFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (5th ed. 2012).

136. *Amnesty Int'l USA*, 133 S. Ct. at 1142.

137. *Id.*

138. *Id.* at 1143.

139. *Id.*

140. *Id.* at 1142.

requirement.[141] Instead of an "objectively reasonable likelihood" of future injury, the Court reiterated that the correct standard was whether the threatened injury was "certainly impending."[142] In rejecting the first theory of injury, the Court stated that the theory was too speculative to satisfy the requirement that an injury be "certainly impending."[143] The Court also rejected the activists' second theory of injury-in-fact, stating that the activists were not allowed to "manufacture standing by choosing to make expenditures based on hypothetical future harm that [was] not certainly impending."[144]

The *Amnesty Int'l USA* decision is not the only time this injury-in-fact standard has been applied to unauthorized government access to data. In an even more recent decision, published in May 2015, the Second Circuit was faced with a similar situation to the one that confronted the Supreme Court two years earlier.[145] The case, *Am. Civil Liberties Union v. Clapper*, was another challenge to government surveillance.[146] Though the fact patterns were largely similar, the Second Circuit distinguished the ACLU plaintiff's situation from that of the plaintiffs in *Amnesty Int'l USA*.[147] Because of that distinction, the Second Circuit court held that the ACLU plaintiffs *did* have injury-in-fact, and were thus able to reach Article III standing.[148]

ACLU v. Clapper involved a challenge to the government's ability to collect data about American citizens under the USA PATRIOT Act of 2001.[149] Prior to the enactment of the Patriot Act, the government was allowed to order certain common carriers (including telephone companies) to provide business records to the government whenever there were "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [wa]s a foreign power or an agent of a foreign power."[150]

141. *Id*. at 1141.

142. *Id*.

143. *Id*. at 1147 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (U.S. 1990)).

144. *Id*. at 1143.

145. *ACLU*, 785 F.3d 787 (2d Cir. 2015).

146. *Id*.

147. *Id*. at 801–02.

148. *Id*. at 802.

149. *See* USA PATRIOT ACT of 2001, Pub. L. No. 107–56, § 215, 115 Stat. 287.

150. *ACLU*, 785 F.3d at 795; *see also* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105–272, § 602, 112 Stat. 2396, 2410–11 (1998).

However, the USA PATRIOT Act of 2001[151] expanded the government's power to not only collect "business records," but also "any tangible things."[152] The amendments also eliminated the restrictions on the types of businesses the government orders could reach.[153] Lastly, the amendments loosened the requirements from requiring "specific and articulable facts" that give reason to believe that the person is a foreign agent, to requiring only a showing that there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[154]

Using this expanded power, the government initiated a program to collect data for foreign surveillance purposes.[155] Under the program, the government ordered telephone companies to provide them "call detail records or 'telephony metadata.'"[156] Though this "metadata" did not include the contents of the phone calls themselves, it did include information that could be considered sensitive and private.[157] The government program, which began in 2006, collected

151. *See* USA PATRIOT ACT of 2001, Pub. L. No. 107–56, § 215, 115 Stat. 287.

152. *ACLU*, 785 F.3d at 795.

153. *Id*. The current statute allows the collection of "any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1).

154. *ACLU*, 785 F.3d at 795; 50 U.S.C. § 1861(b)(2)(A).

155. *ACLU*, 785 F.3d at 795.

156. *Id*.; *see also* Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 BYU L. REV. (forthcoming 2016) (manuscript at 5) (discussing how the Foreign Intelligence Surveillance Court attempted to limit, as much as it could, the government's bulk collection of telephone metadata).

157. *See id*. at 793–94. Telephony metadata is not the contents, or voice conversations, of phone calls themselves, but rather details *about* phone calls. In one of the government orders that was contested in this case, "telephony metadata" was defined as "including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." *In re* F.B.I. for an Order Requiring Prod. of Tangible Things from Redacted, 2013 WL 5741573, at *1 (FISA Ct. Aug. 29, 2013). This information can be used to identify specific devices and users. Then, paired with information about the length of a call, and the number that the user called, it can reveal private information. For example, the government could use the information to discover that a user has called a suicide hotline, alcohol addiction recovery hotline, HIV testing service, or phone-sex service. *See* Brief for Experts in Computer and Data Science, as Amici Curiae Supporting Appellants, *ACLU*, 785 F.3d 787 (No. 14-42), 2014 WL 1118041 at *5–9.

information from *all* calls made both within the United States, and between the United States and abroad.[158]

The plaintiffs in ACLU claimed that the government practice of collecting metadata in bulk, and "on an ongoing daily basis," was not within the scope that Congress authorized in the Patriot Act amendments.[159] Before the Second Circuit could decide the ultimate issue of whether the program was authorized by statute, however, it had to address the threshold question of whether the plaintiffs had Article III standing.[160]

The Second Circuit held that the ACLU plaintiffs *had* alleged sufficient injury to establish Article III standing.[161] Unlike in *Amnesty Int'l* USA, where the plaintiffs "had not established standing because they could not show that the government was surveilling them,"[162] the *ACLU* plaintiffs' claims "require no speculation," since they had already "presented evidence that their data *[we]re* being collected."[163] Therefore, the Second Circuit held that the plaintiffs *did* have injury-in-fact, and eventually held that the government program was not within the Patriot Act's authorized scope.[164]

Taken together, these two cases create a clear, workable standard of addressing injury-in-fact in an unauthorized data-access setting. According to the *Amnesty Int'l USA* standard, if plaintiffs can show that a third party actually accessed their data, the harm is concrete enough to qualify as injury-in-fact because it "requires no speculation."[165] The *ACLU* plaintiffs met this requirement because the government admitted that it had copied the plaintiff's data from the phone companies' records and conducted searches through the database containing the plaintiff's information.[166] On the other hand, if plaintiffs cannot show that a third party actually accessed their personal data, the harm is too speculative to qualify for the injury-in-fact requirement. The *Amnesty Int'l USA* plaintiffs could not meet this

158. *ACLU*, 785 F.3d at 797.
159. *Id.* at 792.
160. *Id.* at 800.
161. *Id.* at 801.
162. *Id.* (quoting *Amnesty Int'l USA*, 133 S. Ct. 1138, 1148–50 (2013)).
163. *ACLU*, 785 F.3d at 801–02.
164. *Id.* at 802, 821.
165. *ACLU, 785 F.3d.* at 801–02.
166. *Id.* at 802.

standard since they were only contesting the amendment to FISA.[167] They did not allege that the government had actually used the amended FISA to access their personal information.[168]

The courts in these two cases had a much different discussion about the standing doctrine and the injury-in-fact requirement than courts in private data breach cases.[169] In *Amnesty Int'l USA* and *ACLU*, instead of speculating on whether unauthorized access to data could cause some uncertain future harm, the courts asked a straightforward question—had the government actually stolen the plaintiffs' data, or not?[170] Asking this question effectively balances the two competing interests behind the data privacy debate. The *Amnesty Int'l USA* standard distinguishes frivolous, unnecessary claims, where the claimants' personal data has not actually been accessed (like the claim in *Amnesty Int'l USA*), from the reasonable claims where personal data has been accessed (similar to that in *ACLU*).

The *Amnesty Int'l USA* standard applies the constitutional doctrine of standing without requiring courts to speculate on potential future harms. Courts can address present facts instead of using their time to calculate the probability of an uncertain, future event.

2. Applying the government standard to private data breach cases

Amnesty Int'l USA and *ACLU* created a strange dynamic in data privacy law. The two cases recognized that plaintiffs could meet the injury-in-fact requirement if the *government* accessed their personal information—even if that information was only metadata. And yet, in private data breach cases such as *Reilly*, the legal system is often unwilling to recognize that a plaintiff can reach injury-in-fact if a *private party* accesses personal information—even if that information includes sensitive financial data.[171] This discrepancy seems awkward and even unfair—to a person who has had his data stolen, it may seem

167. *Amnesty Int'l USA*, 133 S. Ct. at 1148.

168. *Id*.

169. *Compare id*. at 1146–49, and *ACLU,* F.3d at 801–03, *with* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011).

170. *Amnesty Int'l USA*, 133 S. Ct. at 1148; *ACLU*, 785 F.3d at 801.

171. *See supra* Introduction.

that courts care more about who stole his information, than what kind of information was stolen.

Fortunately, the solution to this unusual discrepancy does not require comprehensive change. Instead, the discrepancy can be resolved by using the standard established by *Amnesty Int'l USA* in private data breach actions. Admittedly, some courts in private data breach cases have already discussed the *Amnesty Int'l USA* decision.[172] However, the standard's translation to private cases has been uneasy. Some of the courts using the standard in private cases have claimed that the "certainly impending" language affects the law of standing, while others claim that it does not change the rule.[173]

The reason that the *Amnesty Int'l USA* standard has been an uneasy fit in private cases—and the missing link to its effective use—is that individuals currently have a statutory right against government collection of data, but do not have a statutory right against private collection of data. In an ideal world, legislatures would solve this problem by creating a statutory right to reasonable data security against third party hackers. Legislatures would not necessarily have to create the kind of comprehensive scheme that many scholars have envisioned—they could simply create the right, and formally adopt the *Amnesty Int'l USA* injury-in-fact standard to efficiently apply the standing doctrine.

Even if legislatures do not create a statutory right to reasonable data security, courts may recognize the principle as a common-law right—just as past courts recognized a previously unknown common-

172. *See infra* note 173.

173. *See* Jacobus & Watson, *supra* note 48, at 82–93. Some courts have used *Amnesty Int'l USA*'s language to dismiss private data reach claims, implying that the opinion may have strengthened the requirement that potential future harms be imminent. *See In re* Barnes & Noble Pin Pad Litigation, 2013 U.S. Dist. LEXIS 125730, at *7–12 (N.D. Ill. Sep. 3, 2013); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 875–79 (N.D. Ill. Mar. 12, 2014); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 651–57 (S.D. Ohio 2014). Other courts have cited to the *Amnesty Int'l USA* holding, but still found injury-in-fact, implying (and sometimes stating outright), that the *Amnesty Int'l USA* opinion did not change the law of standing in any significant way. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015); *In re* Sony Gaming Networks and Customer Data Security Breach Litigation, 996 F. Supp. 2d 942, 960–63 (S.D. Cal. 2014); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *14–16 (N.D. Ill. July 14, 2014); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1221–24 (N.D. Cal. Sept. 4, 2014). Overall, it is clear that the inconsistency and uncertainty around private data breach cases has continued.

law right to privacy in tort law.[174] The recognition of this right would make it easy to apply the efficient, clear *Amnesty Int'l USA* standard to private cases.

Recognition of this right is the missing link to allow courts to comfortably apply the *Amnesty Int'l USA* standard. If plaintiffs could show that a third party has already accessed or collected their personal data (for example, by showing attempted draw on an account or the theft of a laptop), they would qualify for the injury-in-fact requirement. On the other hand, if plaintiffs did not claim that a third party had actually accessed or collected their data, they would not satisfy the injury-in-fact standard.

The application of the *Amnesty Int'l USA* standard to private cases would eliminate the need for the difficult and speculative potential-future-injury theory. By applying this standard, courts could better focus on present "cases" and "controversies," rather than searching for hypothetical future injuries.[175] They would be better equipped to handle a modern, digital age where people have to give personal information to third parties on a daily basis—instead of trying to fit the square pegs of pre-digital standards into the round hole of modern reality.

Some may argue that the recognition of an individual right to privacy in data breach cases would result in too much litigation over consumer data breaches. Such a concern may be valid if courts were to recognize an unlimited right to privacy without adopting any standards for discerning between frivolous claims and valid ones. But the *ACLU* decision already demonstrated that the *Amnesty Int'l USA* standard is capable of discerning between serious and frivolous claims.[176]

Even if the recognition of a right to data security results in an increase in data breach litigation, the increase would be a reasonable price to pay if it also increased individual consumer's protection against unauthorized access to sensitive personal data. The American

174. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing for a private right of privacy); Marks v. Jaffa, 26 N.Y.S. 908, 909 (Super. 1893) (an early case that recognized the right to privacy, or that "now the right to life has come to mean the privilege to enjoy life without the publicity or annoyance of a lottery contest waged without authority").

175. U.S. CONST. art. III, § 2.

176. *See supra* Section IV.B.1.

legal system has already proven that it can enforce individual data privacy rights in certain industries, such as healthcare,[177] as long as courts have a workable standard for dividing the reasonable claims from the unreasonable. As long as recognition of the right also came with a workable standard for eliminating frivolous claims, such as the *Amnesty Int'l USA* standard, U.S. courts should be able to handle the claims. Also, many other countries—particularly those in Europe—already have widespread information privacy rights, and have been able to enforce those rights without adverse consequences to their legal systems.[178] The *Amnesty Int'l USA* standard would create a way to strengthen individual privacy rights without causing an unreasonable rise in new data breach claims.

Recognizing a right to protection against unauthorized access to personal data, and combining that right with the standard in *Amnesty Int'l USA*, would allow courts to more closely follow the "cases and controversies" language established by the U.S. Constitution.[179] This method of determining standing would allow courts to address what *has happened*, rather than requiring them to predict what *may happen*. Courts should not be asked to predict the future, but should be able to focus on the allegations already before them. And, as evidenced by the different results in *Amnesty Int'l USA* and *ACLU*, the injury-in-fact standard established by the Supreme Court can differentiate between plaintiffs that meet the injury-in-fact requirement and plaintiffs that do not. The *Amnesty Int'l USA* standard is flexible and strong enough to find the proper balance in determining which suits can be brought.

V. CONCLUSION

The current legal landscape is contradictory when it comes to protecting a consumer's right to data security. The current law allows plaintiffs to bring claims if they have lost data to the government. But

177. *See* Kevin B. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Gap Between Fundamental Privacy Rights and Medical Information*, 19 J. MARSHALL J. COMPUTER & INFO. L. 535, 536–537 (2001); The Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d–1320d-9 (1996); The Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (1970).

178. *See* Ryan Moshell, Comment, . . . *and Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 368–69 (2005).

179. *See* Galbraith, *supra* note 21, at 1385–87.

if they lose data to a private party—even if that data is more sensitive—they often are not allowed to bring their case in court.

This discrepancy is an unintended consequence of the standing doctrine being applied to the digital world. The unwillingness to recognize a right to privacy in personal data creates a substantial hurdle for consumers in private data breach cases to overcome. In response to these doctrines, consumers have turned to creative theories of injury to qualify under the injury-in-fact requirement. These theories, which often require courts to predict the future, are difficult for courts to apply with any degree of consistency.

These problems of applying the standing doctrine to private data breach cases have been discussed by multiple scholars, who have recommended myriad methods of resolving the issue. However, many of these suggestions would be difficult for courts to adopt and apply, and some would still require courts to predict the future. Instead of adopting a complicated solution, the problem can be resolved simply by recognizing a legal right to reasonable protection of data given to third parties in private transactions. If courts recognize this right, they can apply a body of precedent that already deals with unauthorized data collection—the standard established and applied in *Amnesty Int'l USA* and *ACLU*.

By adopting this simple solution, consumers would get a fair chance to bring actions in court if they have their data stolen in a data breach. However, the standard established in *Amnesty Int'l USA* and *ACLU* would also be stringent enough to block frivolous claims when consumers cannot show that their data has been stolen. This standard would allow courts to address private data breach claims fairly, without a need to predict the probability of a potential future harm.

Nick Beatty[*]

[*]JD Candidate, Brigham Young University Law School, 2017.