STAND IN THE PLACE WHERE DATA LIVE: DATA BREACHES AS ARTICLE III INJURIES

JASON S. WASSERMAN*

INTRODUCTION

In the first six months of 2019, organizations suffered over 3,800 data breaches, up fifty-four percent from 2018.[1] Unsurprisingly, identity theft is America's fastest-growing crime.[2] Hackers who coordinate cyberattacks stand to gain significant wealth by either misusing data or selling it to hostile parties, leaving victims vulnerable to fraudulent use of their data.[3] In July 2019, for example, Capital One suffered a breach in which a hacker gained access to approximately 100 million credit card accounts and applications in the United States, including social security and bank account numbers.[4] The Capital One breach likely affected anyone who applied for a credit card in any year from 2005 through 2019.[5]

To respond to data breaches, harmed consumers have some recourse available. The hacker behind a data breach—assuming he or

* J.D. Candidate, Duke University School of Law, Class of 2020. The author would like to thank Professor Jeremy Mullem and the members of the Scholarly Writing Workshop for the helpful feedback on early drafts of this Note.

1. James Sanders, *Data Breaches Increased 54% in 2019 So Far*, TECHREPUBLIC (Aug. 15, 2019, 7:35 A.M.), https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/.

2. United States Postal Inspection Service, *Identity Theft*, UNITED STATES POSTAL INSPECTION SERV. TIPS & PREVENTION, https://www.uspis.gov/tips-prevention/identity-theft/ (last visited Dec. 8, 2019).

3. Thomas Brewster, *Hackers Behind A 770 Million Mega Leak Are Selling 10 Times More Data—But Don't Panic*, FORBES (Jan. 21, 2019, 6:36 A.M.), https://www.forbes.com/sites/thomasbrewster/2019/01/21/hackers-who-leaked-collection-1-are-selling-10-times-more-data-but-you-dont-need-to-panic/#7aeaed477c15; Arjun Kharpal, *Hackers Are Selling Your Data on the 'Dark Web'. . . For Only $1*, CNBC (Sept. 23, 2015, 11:15 A.M.), https://www.cnbc.com/2015/09/23/hackers-are-selling-your-data-on-the-dark-web-for-1.html.

4. *Information on the Capital One Cyber Incident*, CAPITAL ONE, https://www.capitalone.com/facts2019/ (last updated Sept. 23, 2019, 4:15 P.M.).

5. *Id.*

she can actually be found—will likely face federal or state criminal liability and may be forced to pay restitution.[6] But a compromised organization entrusted with the information may also be at fault for facilitating or allowing the unauthorized data exposure, and victims often turn to federal class action suits against such organizations to seek redress.[7] These data breach lawsuits are growing in number each year as more data breaches affect more consumers.[8]

Courts, however, do not even agree on whether or when data breach victims can sue, or in other words, when the victims suffer cognizable legal injuries that create Article III standing.[9] To many courts, plaintiff-victims cannot sue until they prove that they were already, or are absolutely about to be, victims of a subsequent injury occurring long after the original data breach, such as identity theft.[10] Courts differ in defining how much apparent or actual subsequent harm is sufficient for standing, but none to date have held that a data breach alone, regardless of subsequent harm, can cause a cognizable common law injury. The Third Circuit has come the closest, holding that a data breach may cause an inherently cognizable injury when a federal statute is implicated. But no court has extended that approach to state statutory or common law claims.[11] The current array of approaches is based largely on differing interpretations of *Clapper v. Amnesty International USA*, a 2013 Supreme Court case where a class of

6. *E.g.*, *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Jan. 2020), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement; United States Dep't of Justice Off. of Pub. Affairs, *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*, UNITED STATES DEP'T OF JUSTICE (Mar. 15, 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

7. *See* David Balser et al., *INSIGHT: Data Breach Litigation Trends to Watch* ¶ 10, BLOOMBERG LAW (Mar. 4, 2019, 4:01 A.M.), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch ("Some of the most noteworthy data breach litigation developments in 2018 were large consumer class action [data breach] settlements.").

8. *See id.* ("[T]he scale of litigation and regulatory investigations directed towards data security will continue to expand.").

9. *See infra* Part II (discussing circuit split).

10. *See, e.g.*, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58–59, 75 (D.C. Cir. 2019) (discussing cases from other circuits and ultimately finding that plaintiffs had standing); Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft. The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury . . . . By contrast, the First and Third Circuits have rejected such allegations.").

11. *See infra* Parts II.A and II.B (reviewing circuit courts that have found plaintiffs have standing for data breach lawsuits).

individuals alleged that they would be wiretapped by the federal government. In *Clapper*, the plaintiffs did not have standing because the alleged wiretapping was not "certainly impending" and, even more, because those plaintiffs had relied on a chain of speculative assumptions.[12] Some courts have used this precedent in data breach cases to refuse to find standing when plaintiff-victims only allege that because of a data breach, they face an increased risk of, rather than already-occurred instance of, misuse of their personal information.[13] In part, the refusals to find standing are because fraud or other harm following a data breach may take years to manifest and will affect an uncertain number of people.[14]

This Note argues for a different approach from any currently articulated by courts: that data breach victims suffer inherently cognizable legal injuries the moment that their information is disclosed without their consent. A data breach itself, without allegations of future misuse of personal information, generally creates a common law injury. This approach is proper even when a data breach does not lead to subsequent harm. Data breaches fit neatly into the framework of long-recognized privacy torts in which damages are presumed. Data breach victims may also have standing under breach of contract theories. To that end, it is inappropriate to apply *Clapper* to data breach suits because a data breach is generally an adverse event that has already occurred, not a wholly speculative future occurrence. Although enactment of a federal data privacy statute would certainly alleviate standing questions that plaintiff-victims face, there is simply no need for such legislation for standing purposes alone. In essence, if a data breach case is dismissed because the plaintiff-victims fail to plead what are, in effect, meritorious claims, that determination should be under Rule 12(b)(6), at summary judgment, or after trial. Suits should not be dismissed under the false idea that the plaintiff-victims did not suffer cognizable legal injuries.

Holding that data breach plaintiff-victims have standing is consistent with the doctrine of standing. Standing is a separation of

12. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409–10 (2013).

13. *See infra* Part II.C (discussing the third approach in which courts find that plaintiffs do not have standing).

14. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d. Cir. 2011) (discussing the "entirely speculative" nature of alleged data misuse); Lily Hay Newman, *The WIRED Guide to Data Breaches* ¶ 4, WIRED (Dec. 7, 2018, 9:00 A.M.), https://www.wired.com/story/wired-guide-to-data-breaches/ ("Even after a data breach has occurred, though, and an unauthorized actor definitely has your data, you won't necessarily see an immediate negative impact.").

powers principle initially articulated in the early 1920s[15] that ensures courts do not usurp powers of the political branches of the United States government.[16] Essentially, courts decide specific disputes before them about distinct injuries[17] and cannot rule on hypothetical questions. Otherwise, courts would be legislating for future scenarios, thereby infringing the powers reserved to Congress.[18] However, data breach lawsuits pose no such risk. They are based on a past controversy in which victims' information was disclosed without their authorization, and any future harm, such as identity theft, stems from that past event; no conjecture is needed, at least for determining whether victims did in fact suffer harm.[19] Determining the alleged risk of future harm following a data breach is not a question of standing but rather of causation and damages: whether the alleged risk of future harm is proximately tied to the data breach and to what degree the data breach ultimately harmed plaintiffs.[20] For this reason, courts should find that data breach incidents, alleged future harm from them, and costs to mitigate that future harm are sufficient injuries to satisfy standing requirements. Otherwise, victims of data breaches may not even be let into court to adjudicate liability.

In this Note, Part I provides a relevant background on Article III standing. Part II surveys and analyzes the current circuit split over whether and when data breach plaintiffs have standing. Part II also organizes the current approaches to standing into three categories. Then, Part III sets out the Note's main argument, which is that those three existing approaches to standing are improper. And so, Part III

15. *See* Massachusetts v. Mellon, 262 U.S. 447, 488 (1923) ("The party who invokes the [judicial] power must be able to show, not only that the statute is invalid, but that he has sustained or is immediately in danger of sustaining some direct injury as the result of its enforcement, and not merely that he suffers in some indefinite way in common with people generally."); Fairchild v. Hughes, 258 U.S. 126, 129 (1922) ("Plaintiff's alleged interest in the question submitted is not such as to afford a basis for this proceeding. It is frankly a proceeding to have the Nineteenth Amendment declared void.").

16. *Clapper*, 568 U.S. at 408–09.

17. *See* John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1224–25 (1993) (discussing how conjectural, hypothetical, or possible future harm does not meet Article III standing requirements).

18. *See id.* ("We accept the judiciary's displacement of the democratically elected branches when necessary to decide an actual case.").

19. Jennifer M. Joslin, *The Path to Standing: Asserting the Inherent Injury of the Data Breach*, 2019 UTAH L. REV. 735, 749 (2019) ("[A standing] inquiry is unnecessary when courts recognize an injury based on the theft of plaintiffs' personal information, irrespective of potential fraudulent misuse of that information.").

20. *In re* Zappos.com, Inc., 888 F.3d 1020, 1029 (9th Cir. 2018); Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015).

then sets out a "fourth" and proper approach to data breach standing. That is, plaintiffs have federal standing under common law the moment that a data breach occurs. Such immediate standing is appropriate for two primary reasons. First is that data breaches constitute tortious violations of privacy where injuries and damages may be presumed. Second is that data breaches may be violations of obligations to protect data, which are grounded in contract law. Part III then asserts that, because data breaches are in and of themselves injurious, *Clapper*'s "imminence" test for standing does not apply to data breach lawsuits. Finally, Part IV provides policy arguments that support finding that plaintiffs have standing in these cases.

I. ARTICLE III STANDING & RISK OF FUTURE HARM

To litigate in federal courts, a plaintiff must satisfy the constitutional requirement of Article III standing.[21] Standing is grounded in separation of powers principles and ensures that federal courts adjudicate primarily "[c]ases" or "[c]ontroversies."[22] In other words, federal courts may only resolve actual, ongoing disputes between parties.[23] If courts decided questions where no actual controversy existed, they would be "making law" broadly over hypothetical situations, usurping the other federal branches' power.[24]

In practice, standing depends on whether the plaintiff has suffered a cognizable legal injury,[25] which rests on three elements. The plaintiff's alleged injury must be an "injury in fact,"[26] "fairly traceable to the challenged action," and "redressable" by a favorable court ruling.[27] The most important of these elements is establishing the existence of an injury in fact.[28] If the plaintiff cannot show they suffered an injury in

21. Standing is a separate doctrine from Rule 8 pleading standards. Warth v. Seldin, 422 U.S. 490, 500 (1975) ("Although standing in no way depends on the merits of the plaintiffs' contention that particular conduct is illegal, it often turns on the nature and source of the claim alleged."); Wilding v. DNC Servs. Corp., 941 F.3d 1116, 1128 (11th Cir. 2019) ("Whether a plaintiff has Article III standing is a question distinct from whether she has a statutory cause of action.").

22. U.S. CONST. art. III, § 2, cl. 1.

23. Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, & A Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 83 (2017) (citing Warth v. Seldin, 422 U.S. 490, 498 (1975)).

24. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

25. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992) (discussing injuries that create standing as "legally cognizable injuries").

26. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–49 (2016).

27. *Clapper*, 568 U.S. at 409.

28. *Spokeo*, 136 S. Ct. at 1547 (calling establishment of an injury in fact the "first and foremost" element of standing).

fact, traceability and redressability need not be analyzed.[29] Whether an injury in fact exists requires that the alleged harm is (1) particularized, (2) concrete, and (3) actual or imminent.[30]

A. Particularized

An injury is particularized when it affects the plaintiff as a person and individual, rather than as an angry third-party or public observer.[31] A suit to enforce the invasion of a private right, like trespass, presumably passes muster; such private rights inherently belong to individuals.[32] However, a plaintiff cannot bring a suit to enforce a right in the general public interest without also alleging how he or she was personally harmed.[33] For example, a plaintiff cannot sue a government agency for failing to follow a regulation merely because the violation harmed the "public at large."[34] Even when a community in aggregate might practically be affected by a government's regulatory violation, a plaintiff still must demonstrate he or she was personally injured.[35] In data breach cases, a plaintiff's ability to show a particularized injury has not historically been an issue.

B. Concrete

Concreteness entails an independent inquiry into whether an injury is "real, and not abstract," or that it practically and actually exists.[36] Concreteness, as the Supreme Court most recently explained in *Spokeo, Inc. v. Robins*,[37] hinges on both historical practice and whether

29. *See Lujan*, 504 U.S. at 561 ("Since they are not mere pleading requirements but rather an indispensable part of the plaintiff's case, each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." (emphasis in original)).

30. *Spokeo*, 136 S. Ct. at 1548–49.

31. *Id.* at 1548.

32. *See id.* at 1551 (Thomas, J., concurring) ("In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded. Thus, when one man placed his foot on another's property, the property owner needed to show nothing more to establish a traditional case or controversy." (emphasis in original)).

33. *Lujan*, 504 U.S. at 573–74 ("We have consistently held that a plaintiff raising only a generally available grievance about government—claiming only harm to his and every citizen's interest in proper application of the Constitution and laws, and seeking relief that no more directly and tangibly benefits him than it does the public at large—does not state an Article III case or controversy.").

34. *Spokeo*, 136 S. Ct. at 1551–52 (Thomas, J., concurring).

35. *Id.*

36. *Id.* at 1548–49 (majority opinion) (internal quotation marks omitted).

37. *Id.* at 1548–50.

Congress defined a particular right via statute.[38] And, although a tangible injury like physical harm is quickly recognized as concrete, an injury need not be tangible to be concrete. For example, violations of constitutional free speech and free exercise rights are concrete injuries.[39] Similarly, if a statute mandates that certain information be publicly available, and individuals cannot obtain that information, a concrete harm exists.[40]

Recently, the Supreme Court in *Spokeo* laid out a framework for determining the concreteness of injuries for statutory violations.[41] In *Spokeo*, a "people search engine" named Spokeo, Inc. had disseminated information about the plaintiff, Thomas Robins, that was allegedly inaccurate.[42] Robins subsequently sued Spokeo under the federal Fair Credit Reporting Act, theorizing that his statutory right to handle his credit reporting information was violated.[43] Initially, the district court dismissed Robins's suit for a lack of standing, but the Ninth Circuit later found that Robins did have standing because he suffered an individualized and particularized harm.[44] However, the Supreme Court ultimately held that the Ninth Circuit's analysis was incomplete because it had failed to consider the "concreteness" of Robins's alleged injury, and so the Court remanded the case for a new and full standing analysis.[45] Under *Spokeo*, Congress may, via statute, create new cognizable legal injuries,[46] but a bare procedural violation may result in no actual harm. Therefore, a plaintiff does not automatically show concrete injuries every time a statute is violated.[47] Courts must take care to examine a plaintiff's theory of harm.

---

38. *Id.* at 1549.
39. *Id.*
40. *Id.* (citing Fed. Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998)).
41. *Id.* at 1550.
42. *Id.* at 1544.
43. *Id.*
44. *Id.* at 1544–45.
45. *Id.* at 1545.
46. *Id.* at 1549 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992)) ("Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'" (emphasis in original)); Warth v. Seldin, 422 U.S. 490, 514 (1975) ("Congress may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute.").
47. *Spokeo*, 136 S. Ct. at 1549 ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.").

After the Supreme Court remanded *Spokeo* for the Ninth Circuit to reconsider standing, the Ninth Circuit offered one possible interpretation of the Supreme Court's framework using a two-part test. First, courts must ask whether Congress established the statute in question to protect concrete interests, as opposed to merely procedural rights; and second, if the answer to the first question is affirmative, courts must check whether the violation in question harms or presents a risk of material harm to those concrete interests.[48] Notably, the Supreme Court in *Spokeo* also confirmed that the mere "*risk* of real harm" could be one such concrete injury.[49] *Spokeo* thus provides insight into how courts should examine data breach cases. The concreteness of an alleged injury, and therefore standing, depends largely on which injuries a plaintiff alleges, congressional purposes for any statutory provision in question, and the nature of common law rights violated.[50]

C. Actual or Imminent

Finally, an alleged injury must be "actual or imminent."[51] That is, the alleged injury must have already occurred, be ongoing, or, if an injury is alleged to be in the future, it must be more than just "possible."[52] This requirement is particularly relevant in data breach cases when allegations include the risk of future identity theft. In *Clapper v. Amnesty International USA*, the Supreme Court outlined when an injury might be actual or imminent.[53] *Clapper*'s facts differ from those of data breach cases, but it is nonetheless an important case because some circuit courts choose to rely on it in data breach suits.

In *Clapper*, a group representing human rights, labor, legal, and media organizations challenged the constitutionality of Section 702 of the Foreign Intelligence Surveillance Act.[54] Section 702 authorized the United States to undertake warrantless wiretapping for foreign intelligence purposes.[55] The plaintiffs sued the United States before

48. Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017) ("[W]e thus ask: (1) whether the statutory provisions at issue were established to protect his concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."). Ultimately, the Ninth Circuit found that Robins had standing. *Id.* at 1118.

49. *Spokeo*, 136 S. Ct. at 1549 (emphasis added).

50. *Id.* at 1549–50.

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

52. *Id.*

53. *Id.* at 401, 408–09.

54. *Id.* at 401, 406–07.

55. *Id.* at 403.

actually having their communications intercepted and merely alleged there was an "objectively reasonable likelihood" that their communications would be acquired "at some point in the future."[56] The Supreme Court held the plaintiffs lacked standing.[57] The plaintiffs had no knowledge that the government had "targeted" their particular communications, nor was there any past occurrence of harm.[58] Accordingly, the plaintiffs had not suffered actual or imminent harm but merely unsubstantiated fears.[59]

The Court explained that the imminence requirement for an injury in fact is "a somewhat elastic concept," but an alleged future injury cannot be stretched so far to be wholly speculative.[60] If so, claims of risk of future injury, or preventative measures to address thereof, are insufficient.[61] The Supreme Court obliquely described two potential standards for claimed future harms to satisfy the imminence requirement. The first and stricter standard is that an injury must be "certainly impending."[62] The second potential standard, however, merely requires plaintiffs to show a "substantial risk" that harm will occur, even when it may not be certain that harm will ever come about.[63] Under either potential standard, plaintiffs cannot simply allege an "attenuated chain of inferences" that lead to some future harm.[64]

It is not clear when exactly the "substantial risk" standard applies, even to circuit courts that have split on how to understand *Clapper*'s framework. In part, the uncertainty is because the Court discussed the possibility that the two standards are not entirely separate.[65] The Court stated that "[i]n some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[66] But "to the extent that the 'substantial risk' standard is relevant and is distinct from

56. *Id.* at 407.
57. *Id.* at 420, 422.
58. *Id.* at 410.
59. *Id.* at 420, 422.
60. *Id.* at 409 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 565 n.2 (1992)) ("Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." (emphasis in original)).
61. *Id.* at 401, 409.
62. *Id.* at 401.
63. *Id.* at 414 n.5.
64. *Id.*
65. *Id.*
66. *Id.*

the 'clearly impending' requirement, respondents fall short."[67] The *Clapper* Court applied the "certainly impending" standard, but application to other areas of law is uncertain. The data breach circuit split is in part over whether *Clapper* governs those cases and, if so, which standard applies.

II. CURRENT APPROACHES TO DATA BREACH STANDING

Circuit courts have split on when plaintiffs bringing claims following data breaches have standing.[68] The split concerns whether—and how much—an increased risk of future harm following a data breach is an injury in fact sufficient for standing. Different circuits utilize one of three contrasting approaches. However, each approach is analytically improper in virtually all data breach cases. Even when courts have determined that data breach plaintiff-victims have standing, which is the correct result, the means and reasoning under which they do so are improper. And so, this Note suggests in Part III a fourth approach not currently endorsed by any court.

The first approach is that a data breach may constitute an "actual" injury but only when plaintiffs bring claims under a federal statute. Under this approach, *Clapper* need not apply, and it is unnecessary to evaluate the imminence of future harm.[69] The second approach is a lenient standard of "substantial risk" analysis: A data breach victim may have suffered an injury in fact because, although plaintiffs must show they face subsequent imminent harm, that bar is low.[70] Third is that a data breach alone is not evidence of an injury: A plaintiff must show conclusively that a given data breach has led to looming or actual identity theft, fraud, blackmail, or other harm.[71]

A. First Approach: A Data Breach Can Be Inherently Injurious

The first approach, currently adopted by only the Third Circuit, is that data breach plaintiffs might have standing for actual injuries if a

67. *Id.*

68. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) ("The courts of appeals have evidenced some disarray about the applicability of this sort of 'increased risk' theory in data privacy cases.").

69. To date, this first approach has only been advanced by the Third Circuit. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 629, 640 (3d Cir. 2017).

70. To date, this second approach has been followed at least once by the Fourth, Sixth, Seventh, Ninth, and District of Columbia Circuits. *See infra* Part II.B.

71. To date, this third approach has been followed at least once by the Second, Third, Fourth, Eighth, and Eleventh Circuits. *See infra* Part II.C.

federal statute is implicated. In *In re Horizon Healthcare Services*, the Third Circuit held that being the victim of a data breach can be an injury in and of itself, sufficient for standing, if the cause of action is under a federal statute like the Fair Credit Reporting Act of 1970 ("FCRA").[72] The majority opinion did not cite *Clapper*.[73] Instead, the court relied on *Spokeo*, noting that Congress has the power to define injuries with legislation, in which case a substantive statutory violation constitutes cognizable harm.[74] In *Horizon*, thieves stole two laptops containing credit card information from a health insurer.[75] Plaintiffs brought suit under FCRA, which requires that consumer reporting organizations take reasonable steps to ensure the accuracy and integrity of consumer information.[76] The court found that the plaintiffs had standing regardless of whether the disclosure of information would cause future harm because the plaintiffs alleged "unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent."[77] That is, "[e]ven without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a *de facto* injury."[78]

The court compared data breaches to privacy torts in explaining why a FCRA violation was inherently an injury in fact. The court explained that "with privacy torts, improper dissemination of information can itself constitute a cognizable injury."[79] That invasion of privacy, which is an intangible harm, "has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[80] Congress, in enacting FCRA, sought to protect against injuries closely related to that long-recognized intangible harm, so a substantive FCRA violation was inherently sufficient for standing.[81]

The Third Circuit subsequently clarified the *Horizon* holding. For plaintiffs to have de facto standing under a federal statute, they must allege that the statute in question protects rights "of the same character as a previously existing" injury.[82] In a data breach case, that means the

72. The Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681–1681x (2018).
73. *Horizon*, 846 F.3d at 634.
74. *Id.* at 638, 640.
75. *Id.* at 630.
76. *Id.* at 631.
77. *Id.* at 640.
78. *Id.* at 629.
79. *Id.* at 638–39.
80. *Id.* at 639–40 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
81. *Id.*
82. Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019).

statute must protect against the unauthorized disclosure of personal information to a third party.[83]

The *Horizon* court also limited this standing approach to federal statutory violations because common law claims were not at issue.[84] The court stated that despite its discussion of privacy torts, it was "not suggesting that Horizon's actions would give rise to a cause of action under common law."[85] In particular, "[n]o common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive."[86] However, even if *Horizon* had involved common law claims, it is unlikely that the Third Circuit would have held differently. Several years before *Horizon*, the Third Circuit held in a different data breach case that plaintiffs who brought common law claims did not have standing.[87] Examining the Third Circuit's cases together, it is left open, albeit unlikely, that the court might consider a data breach as creating a de facto injury under common law.

B. Second Approach: Proving Imminence is a Low Bar

Second, other courts have found standing for another reason: that although data breach plaintiffs must still demonstrate that subsequent future harm is imminent, the burden is low.[88] These courts use the "substantial risk" standard from *Clapper* and generally find that plaintiffs face a substantial risk of identity theft or fraud as soon as hackers hold stolen information, regardless of whether the claims are statutory or under common law.[89] Pursuant to this approach, there is "no need to speculate"[90] whether plaintiffs have standing because of the "obvious potential" for misuse of stolen data.[91] As the Seventh

83. *Id.*

84. *See Horizon*, 846 F.3d at 639–40 (discussing statutory, rather than common law, harms and explicitly denying that the opinion's standing analysis necessarily applies to common law claims).

85. *Id.* at 639.

86. *Id.*

87. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

88. *E.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017); Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d. 1197, 1214 (N.D. Cal. 2014)).

89. Although these courts take a variety of approaches, what they hold in common is that plaintiffs have standing when they allege that a data breach caused them an increased risk of future harm. *E.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1024, 1027–28 (9th Cir. 2018); *Attias*, 865 F.3d at 628–29; Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 388 (6th Cir. 2016).

90. *Remijas*, 794 F.3d at 693.

91. *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58, 60 (D.C. Cir. 2019).

Circuit noted, "[w]hy else would hackers break into a store's database and steal consumers' private information?"[92] The purpose of a hack is presumably to sooner or later commit a fraudulent act, leading to a clear risk of harm.[93] This approach tends to find that plaintiffs have standing, which is the correct result. But the approach still examines whether plaintiffs will suffer injuries subsequent to the data breach, which is improper reasoning.

For example, the Sixth Circuit in *Galaria v. Nationwide Mutual* held that plaintiffs had standing for FCRA violations and common law claims because there was imminence of future harm as soon as the plaintiffs' information was "in the hands of ill-intentioned criminals."[94] In *Galaria*, hackers breached Nationwide, a large insurance and financial services company.[95] The Sixth Circuit found that the plaintiffs had standing despite that it was not "literally certain" the plaintiffs' data would be misused.[96] Similarly, in *Remijas v. Neiman Marcus*, the Seventh Circuit found that the plaintiff had standing following a breach of Neiman Marcus, a luxury department store. The court found that the plaintiffs had standing because "the risk that Plaintiffs' personal data will be misused by the hackers . . . is immediate and very real."[97] Additionally, some of the plaintiffs had already suffered fraudulent charges on their credit cards by the time of the lawsuit,[98] which helped indicate that those who had not yet faced fraudulent charges almost certainly would soon.[99]

Under this approach, plaintiffs may have standing even when they plead that the precise amount of harm may not be clear for "some time."[100] For example, in the Ninth Circuit case *In re Zappos.com*, a hacker stole credit card information of over 24 million individuals from Zappos.com; the plaintiffs then alleged that they "[might] not see the full extent of identity theft or identity fraud for years."[101] Yet, the court

92. *Remijas*, 794 F.3d at 693.
93. *Id.*
94. *Galaria*, 663 F. App'x. at 388.
95. *Id.* at 386.
96. *Id.* at 388.
97. *Remijas*, 794 F.3d at 693 (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d. 1197, 1214 (N.D. Cal. 2014)).
98. *Id.* at 689–90.
99. *Id.* at 693–94 ("The plaintiffs are also careful to say that only 9,200 cards have experienced fraudulent charges *so far*; the complaint asserts that fraudulent charges and identity theft can occur long after a data breach." (emphasis in original)).
100. *In re* Zappos.com, Inc., 888 F.3d 1020, 1028–29 (9th Cir. 2018).
101. *Id.*

found that the plaintiffs had standing regardless of potential delay in harm because the thieves already had "all the information . . . needed to open accounts or spend money in the plaintiffs' names."[102]

Additionally, the type of data exposed—that is, whether it is particularly sensitive to misuse—may matter.[103] The *Zappos* court, for example, found it important that credit card numbers are particularly vulnerable to identity theft.[104] And in *In re U.S. Office of Personnel Mgmt.*,[105] the D.C. Circuit found that the plaintiffs had standing following a hack of the United States Office of Personnel Management in part because social security numbers and fingerprint records were especially sensitive to misuse.[106]

C. Third Approach: An Increased Risk of Harm After a Data Breach is Not an Injury in Fact

The third approach used by courts is that a data breach by itself cannot generally indicate a cognizable injury regardless of whether there is an increased risk of future misuse. Courts that refuse to find standing for claims of increased risk of future harm tend to do so because plaintiffs rely on too many assumptions, making an actual injury "hypothetical."[107] To these courts, victims' credit card and bank statements may be "exactly the same today as they would have been had [a] database never been hacked."[108] That is, a data breach itself constitutes mere means to real harm.[109]

In *Beck v. McDonald*, the Fourth Circuit found that the plaintiffs did not have standing after the data breach of a hospital because the plaintiffs could not show their information was or would be misused.[110]

---

102. *Id.* at 1023, 1026.

103. *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58, 60 (D.C. Cir. 2019); *Zappos*, 888 F.3d at 1027–28.

104. *Zappos*, 888 F.3d at 1027–28 (discussing the particular sensitivity of credit card information).

105. Plaintiffs brought claims under the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq.* (2012) (repealed 2014), and the Federal Information Security Modernization Act of 2014 ("FISMA 14"), 44 U.S.C. §§ 3551 *et seq.* (2018). Both acts provided required software security steps for federal agencies. *Office of Pers. Mgmt.*, 928 F.3d at 51.

106. *Office of Pers. Mgmt.*, 928 F.3d at 49, 58, 60. The court also found standing in part because some plaintiffs had already suffered harm.

107. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

108. *Id.* at 45.

109. *See, e.g.*, Whalen v. Michaels Stores, Inc., 698 F. App'x. 89, 91 (2d Cir. 2017) (finding a data breach of a brick-and-mortar retailer does not itself constitute an injury in fact for individuals whose information was exposed).

110. Beck v. McDonald, 848 F.3d 262, 275–76 (4th Cir. 2017).

The plaintiffs relied on the Privacy Act of 1974, which applies to federal agencies.[111] A Veterans Affairs Medical Center had lost personal information of 7,400 patients after a laptop went missing, likely from theft.[112] The Fourth Circuit found that although a violation of the Privacy Act was potentially a concrete injury, the plaintiffs did not demonstrate that future harm was imminent.[113] Plaintiffs neither met the "certainly impending" threshold for harm nor the lesser standard of "substantial risk" of future harm.[114] It was not enough that objectively thirty-three percent of the plaintiffs would suffer identity theft—a fact that the court accepted as true for the analysis of standing—because the other sixty-six percent "w[ould] suffer no harm."[115] To find standing, the court would have had to make unfounded assumptions in an "attenuated chain."[116]

Similarly, in *In re SuperValu*, the Eighth Circuit refused to hold that the plaintiffs had standing after hackers stole credit card information from computer systems of over 1,000 SuperValu grocery stores.[117] Plaintiffs sued the grocery store chain under state statutory and common law claims.[118] The court found that although the plaintiffs demonstrated the possibility of future harm, mere possibility was not enough.[119] Credit card information did not alone indicate a high likelihood of fraudulent use because no accompanying "personally identifying information," such as birth dates or social security numbers, was stolen.[120] Accordingly, there was little risk that a bad actor could "open unauthorized accounts in the plaintiffs' names."[121] The court thought that there was still a risk of "unauthorized charges" using existing credit card accounts, but that risk was not enough to indicate a "substantial risk" of harm sufficient for standing.[122]

In *Wilding v. DNC Services Corp.*, the Eleventh Circuit found that being the victim of a data breach does not alone mean plaintiffs have

111. 5 U.S.C. § 552a (2018); 5 U.S.C. § 552(f) (2018).
112. *Beck*, 848 F.3d at 267.
113. *See id.* at 271 n.4 (discussing that some other circuits, following *Spokeo*, have found violation of a privacy statute to be a *de facto* concrete injury).
114. *Id.* at 268, 275–76.
115. *Id.* at 268.
116. *Id.* at 275.
117. *In re* SuperValu, Inc., 870 F.3d 763, 765 (8th Cir. 2017).
118. *Id.* at 767.
119. *Id.* at 771–72.
120. *Id.*
121. *Id.*
122. *Id.*

standing under common law.[123] The court stated that "[t]here is admittedly some support for the notion that the mere violation of a state-law right satisfies Article III even in the absence of an identifiable injury."[124] But nonetheless, "[w]e require plaintiffs asserting violations of state-created rights to demonstrate a concrete injury; the defendant's violation of those rights is not enough."[125] In *Wilding*, registered Democrats and donors to the Democratic National Committee ("DNC") sued the DNC after hackers breached its servers during the 2016 Presidential election.[126] The *Wilding* plaintiffs formed multiple classes, one of which alleged a simple breach of fiduciary duty.[127] That class did not have standing.[128]

D. Analyzing the Split

A few trends emerge from the circuit split regarding standing in data breach cases.[129] First, plaintiffs tend to bring suits under state law, grounded in federal diversity jurisdiction, rather than under federal statutes.[130] This is likely due to a lack of federal statutory causes of action available, leading to difficulty finding federal question jurisdiction.[131] For example, FCRA only applies to consumer reporting agencies,[132] and the Privacy Act only applies to federal agencies.[133]

Second, however, cases that do hinge on federal statutes fare significantly better than those that hinge on state law. Plaintiffs had standing in all but one case where a federal statute was in question. *Beck* is the one case based on a federal statute where the court did not find that plaintiffs had standing, but *Beck* is perhaps unique. In *Beck*, the Fourth Circuit refused to find that plaintiffs had standing for claims brought under the Privacy Act after a laptop containing sensitive

123. Wilding v. DNC Servs. Corp., 941 F. 3d 1116, 1130 (11th Cir. 2019).
124. *Id.* at 1131.
125. *Id.*
126. *Id.* at 1122–23.
127. *Id.* at 1130.
128. *Id.* A different class of plaintiffs that alleged actual financial loss *did* have standing because "[s]uch economic harm is a well-established injury for purposes of Article III standing." *Id.* at 1125. In this way, the court seemingly followed the second approach of the circuit split. *Supra* Part II.B.
129. The analysis of Part II.D is based on each cited case reviewed in Parts II.A–C.
130. This finding based on each cited case reviewed in Parts II.A–C, plus prior or ancillary precedent not discussed.
131. 28 U.S.C. § 1331 (2018).
132. 15 U.S.C. § 1681(b) (2018).
133. 5 U.S.C. § 552a (2018) (laying out requirements for agencies); 5 U.S.C. § 552(f) (2018) (defining "agency").

personal information went missing.[134] But the Fourth Circuit later found that plaintiffs had standing in *Hutton*, a case with state law claims and strong evidence of impending future harm. However, the cases can be reconciled. The court explained, "[i]n *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes . . . had been stolen, but the information contained therein had not been misused."[135] Moreover, the court "concluded that the threat was speculative because 'even after extensive discovery' there was 'no evidence that the information contained on [a] stolen laptop [had] been accessed or misused or that [the plaintiffs had] suffered identity theft.'"[136] Thus, it seems the *Beck* plaintiffs did not have standing from a lack of specificity in their pleadings and scant evidence after discovery.[137] Therefore, the Fourth Circuit may find that plaintiffs have standing if they allege more than just theft itself.[138]

Also notable is that the Third Circuit has both granted and denied standing for data breach cases alleging a risk of future injury. These cases can also be reconciled. In *Ceridian*, the court refused to find that standing existed for state common law claims stemming from a cyberattack because even with some possibility of future harm, the risk was too speculative.[139] But the court found that plaintiffs had standing in *Horizon*, a case brought after suspected laptop theft, which hinged on FCRA.[140] These cases taken together indicate that the Third Circuit affords great weight to decisions of Congress to create federal causes of action via legislation.

III. THE PROPER FRAMEWORK FOR STANDING

All three current approaches to standing are improper because a data breach causes an inherently cognizable legal injury the moment that information is exposed or acquired. In *Horizon*, the Third Circuit came close to this approach but only when plaintiffs alleged harm under the FCRA federal statute.[141] A more proper approach would extend that framework to common law claims: that "the unauthorized

134. Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).
135. Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 621–22 (4th Cir. 2018).
136. *Id.* at 622.
137. *Id.*
138. *Beck*, 848 F.3d at 275.
139. Reilly v. Ceridian Corp., 664 F.3d 38, 41, 46 (3d Cir. 2011).
140. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639 n.20 (3d Cir. 2017).
141. *See supra* notes 72–86 and accompanying text.

dissemination of personal information . . . causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm."[142] This approach is in line with long-recognized tort law and contract law principles. Additionally, because a data breach itself causes a cognizable injury, *Clapper*'s framework requiring plaintiffs to show that future harm is imminent should not govern data breach cases. *Clapper* was about injuries based entirely on a speculative future event. However, a data breach case is about a past event: the unauthorized disclosure of information. Finding standing through this approach also upholds standing's main purpose of separation of powers.

A. Unauthorized Disclosure of Information is an Injury in and of Itself

After hackers access sensitive personal information, the initial reaction of victims may, unsurprisingly, be alarm.[143] Indeed, in any data breach, an unauthorized third-party accesses a victim's private information.[144] In some cases, merely a social security number with its corresponding name can be enough for a bad actor to commit identity theft.[145] However, if data breaches are harmful because of the fraud to which they lead, one could argue that there is no harm in a data breach itself. It may be unsettling when information that was expected to be kept confidential by its steward is exposed. Still, to build a case for why data breach plaintiffs have standing, that exposure must be contextualized under a legal theory of harm. This Section lays such a framework and explains why a data breach is an inherently cognizable injury under common law tort and contract regimes.

1. Data Breaches as Tortious Invasions

Experts maintain that "[i]t's totally reasonable to assume that your social security number has been compromised at least once, if not many times,"[146] and that "repercussions of a breach can be very delayed,

142. St. Pierre v. Retrieval-Masters Creditors Bureau, Inc., 898 F.3d 351, 357 (3d Cir. 2018) (quoting *Horizon*, 846 F.3d at 639).

143. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 49 (D.C. Cir. 2019) ("[T]he data breaches affected more than twenty-one million people. Unsurprisingly, given the scale of the attacks and the sensitive nature of the information stolen, news of the breaches generated not only widespread alarm, but also several lawsuits.").

144. Symantec, *What Is a Data Breach?*, NORTON, https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (last visited Dec. 9, 2019).

145. Paul Wagenseil, *What to Do After a Data Breach*, TOM'S GUIDE (Apr. 15, 2019), https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html.

146. Suzanne Rowan Kelleher, *Everyone's Social Number Has Been Compromised. Here's*

sometimes not fully manifesting for years."[147] It would follow, then, that many individuals have already had their social security number compromised yet are unaware, unflinching, and unharmed. Under these circumstances, perhaps it might be correct to view a data breach as not itself an injury in fact. The common law, after all, does not recognize unconsented information disclosure as injurious unless the disclosure is "harmful to one's reputation or otherwise offensive."[148]

However, the mere exposure of information from a data breach is intuitively offensive because sensitive private facts are disseminated, which may cause anxiety over the threat of looming injuries or embarrassment.[149] This "value of mental suffering" has long been recognized in American law, a seminal conception of which was asserted in 1890[150] in *The Right to Privacy*.[151] In that essay, Justice Louis Brandeis and Samuel Warren argued that the invasion of privacy, like defamation, should be actionable.[152] Indeed, modern privacy torts,[153] including "unreasonable publicity" and "breach of confidence," protect against such exposure.[154] Both of those torts are actionable so long as pleadings allege that a third party gained unauthorized access to the

How to Protect Yourself., FORBES (Aug. 1, 2019, 1:42 P.M.), https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/#4848379a29ac.

147. Lily Hay Newman, *supra* note 14, at ¶ 4.

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

149. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 964 (1989) ("An intrusion on privacy is *intrinsically* harmful because it is defined as that which injures social personality." (emphasis in original)).

150. RESTATEMENT (SECOND) OF TORTS § 652A (2016) ("The right of privacy has been defined as the right to be let alone. Prior to 1890 no English or American court had ever expressly recognized the existence of the right, although there were decisions that in retrospect appear to have protected it in one manner or another.").

151. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

152. *Id.* at 218–19.

153. RESTATEMENT, *supra* note 150, § 652A (enumerating the four ways in which privacy is invaded); David A. Elder, *Privacy Torts* § 1:1 (2016).

154. *See* Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019) (describing unreasonable publicity and breach of confidence as "[h]arms actionable under traditional privacy torts"); *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 638–39 (3d Cir. 2017) ("And with privacy torts, improper dissemination of information can itself constitute a cognizable injury."); Post, *supra* note 149, at 964 ("[T]he privacy tort enables a plaintiff to make out his case without alleging or proving any actual or contingent injury, such as emotional suffering or embarrassment. The privacy tort shares this profile with other torts which redress 'dignitary harms.'"); Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1455 (1982) ("[T]he tort can be defined in general terms as the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship.").

plaintiffs' information.[155] A data breach is no different. A hacker is an intruding third party who gains unauthorized access to plaintiffs' information through a steward entrusted with it.[156]

The Supreme Court confirmed in *Doe v. Chao* that for "privacy and defamation torts," damages are "presumed . . . without reference to specific harm."[157] Logically, if damages are presumed, then so should be standing.[158] The Third Circuit even noted in *Horizon* that because damages to one's privacy are "uncertain and possibly unmeasurable," privacy tort victims may be awarded money damages that are "calculated without proving actual damages."[159] To that end, courts should, at least for standing purposes, presume injury regardless of how plaintiffs might label their injuries, whether as certain torts or simply negligence.[160]

The suggested limiting principle to this approach is that data breach plaintiffs must still factually show either that they lost control over their information or that a bad actor gained unauthorized access to it. This threshold will almost always be met when a case arises from a hack, which is by definition unauthorized access to data.[161] But plaintiffs in laptop theft cases may face greater burdens. For example, in a case of laptop theft where personal information is stored on the laptop, privacy is invaded as soon as the laptop is in the hands of an unintended recipient.[162] Then, individuals whose information is accessible within

155. *Kamal*, 918 F.3d at 114; *Horizon*, 846 F.3d at 638–39; Vickery, *supra* note 154, at 1455.

156. *See* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 627–28 (2018) (arguing that an organization entrusted with data is a "data confidant" with fiduciary duties).

157. Doe v. Chao, 540 U.S. 614, 621 (2004); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("[T]he law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure.").

158. *See* Lauren E. Willis, *Spokeo Misspeaks*, 50 LOY. L.A. L. REV. 233, 249 (2017) (arguing that "the Supreme Court has never blinked at" the presumption of damages in libel and defamation suits, and so "the question of standing" need not be raised).

159. *Horizon*, 846 F.3d at 638–39.

160. *E.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 767 (8th Cir. 2017) (mentioning that the plaintiffs raised negligence claims); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696–97 (7th Cir. 2015) (addressing claims that the defendant was negligent in protecting the plaintiffs' information).

161. Tripwire Guest Authors, *The Evolution of Hacking*, TRIPWIRE.COM (Aug. 17, 2016), https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/.

162. *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) ("[In *Krottner*] we held that employees of Starbucks had standing to sue the company based on the risk of identity theft they faced after a company laptop containing their personal information was stolen."); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Here, Plaintiffs-Appellants have alleged

have suffered a cognizable injury.[163] But if a thief steals a laptop that does not actually store information—e.g., if the information is stored on a cloud server—[164] the laptop theft alone might not implicate a cognizable injury because no personal information was exposed, acquired, or otherwise accessed.[165] Therefore, with a hack, it will generally be clear whether a bad actor accessed private information.[166] But standing in laptop theft cases may not be immediately clear, depending the facts at hand.[167] This limiting factor does not cut against a court's ability to label a data breach as a common law injury; instead, it merely recognizes that there might be cases where a data breach is factually difficult to establish as having occurred at all.

Once it is established the plaintiffs' information was accessed without authorization, any alleged "increased risk of future harm" stemming from that data breach is harm anchored to and extending from it.[168] For example, plaintiffs may allege that because of a data breach, they face an increased risk of identity theft.[169] Thus, potential future harm simply adds to the harm from the data exposure itself. Courts should therefore evaluate that likelihood of future harm as an inquiry into causation and damages during later phases of litigation: Did the data breach proximately cause the alleged future harm, and if so, then how much is that predicted harm worth?[170] The Ninth Circuit took this approach in *Zappos*, stating "[t]hat hackers might have stolen

a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.").

163. *Horizon*, 846 F.3d at 642 (Schwartz, J., concurring).

164. *See* Wendy Zamora, *Should You Store Your Data in the Cloud?*, MALWAREBYTES LABS (July 26, 2018), https://blog.malwarebytes.com/101/2016/04/should-you-store-your-data-in-the-cloud/ (explaining that data stored in the "cloud" is not physically on a single computer).

165. The plaintiffs in *Beck*, where the Fourth Circuit found that the plaintiffs did not have standing, may still not have standing even under the approach proposed in this Note. Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) ("[W]e concluded [in *Beck*] that the threat was speculative because 'even after extensive discovery' there was 'no evidence that the information contained on [a] stolen laptop [had] been accessed or misused or that [the plaintiffs had] suffered identity theft.'").

166. *E.g.*, *Zappos*, 888 F.3d at 1023 (noting that the defendant told customers that their personal information had been stolen); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 386 (6th Cir. 2016) (noting that the defendant acknowledged the data breach occurred and advised customers to monitor their bank statements to prevent misuse of stolen data).

167. *Hutton*, 892 F.3d at 622.

168. *See Horizon*, 846 F.3d at 642 ("While [loss of privacy] may or may not be sufficient to state a claim for relief under Fed. R. Civ. P. 12(b)(6), the intangible harm from the loss of privacy appears to have sufficient historical roots to satisfy the requirement that Plaintiffs have alleged a sufficiently concrete harm for standing purposes.").

169. *See supra* notes 94–99 and accompanying text (discussing circuit cases in which plaintiffs alleged an increased risk of identity theft or other harm as caused by data breaches).

170. *Id.*; *Zappos*, 888 F.3d at 1029.

Plaintiffs' [personally identifying information] in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages."[171]

Perhaps more importantly, data breach victims may buy prophylactic services to protect themselves from the risk of identity theft.[172] Victims, for example, may buy credit monitoring services in direct response to their credit card numbers being compromised.[173] Such time and money spent to "set things straight" indicates an injury in fact.[174] Any court that may have trouble concluding that unauthorized data disclosure is a cognizable injury should surely, once the plaintiffs allege actual purchase of mitigation expenses, find standing. These mitigation expenses, if reasonable, are not manufactured or self-imposed.[175] They reflect non-speculative, "actual injuries" because the harm already occurred, and the risk of future fraud is "sufficiently immediate to justify mitigation efforts."[176] These expenses can include costs to investigate and monitor potential fraud, to cancel and re-issue credit cards,[177] or simply "the time value of money" and legwork used to stop the bleeding caused by a data breach.[178]

Additionally, the hacker and the compromised steward of information may both be at fault for plaintiffs' injuries.[179] Whether the defendant actually violated the law or whether an ill-intentioned hacker is solely at fault is not a question of Article III standing.[180] And,

171. *Zappos*, 888 F.3d at 1029.

172. *In re* 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1256–57 (M.D. Fla. 2019).

173. *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) ("[T]he value of one's own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries can justify money damages, just as they support standing.").

174. *Id.*

175. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (confirming that "the time and money spent resolving fraudulent charges are cognizable injuries for Article III standing" and that expenses to replace cards and purchasing credit monitoring services are reasonable mitigation costs after a data breach).

176. *Id.*

177. *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d. 1150, 1160 (N.D. Ga. 2019).

178. *Dieffenbach*, 887 F.3d at 828.

179. *See* Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015) ("The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue." (emphasis in original)).

180. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017) ("Here, by contrast, an

to the extent these fault determinations matter for standing, they go to traceability, not whether a plaintiff suffered an injury in fact. The Sixth Circuit in *Galaria* noted that "[a]lthough hackers are the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because [the defendant] allegedly failed to secure the sensitive personal information entrusted to its custody," and "[t]h[o]se allegations meet the threshold for Article III traceability."[181] If a court decides that the risk of identity theft or fraud is not the compromised organization's fault, that determination will be made after standing has been established.[182] Therefore, if a data breach lawsuit must be dismissed, it should be dismissed on the merits under Rule 12(b)(6),[183] on summary judgment[184] or after a trial, not for the plaintiffs' lack of standing.[185]

Relatedly, some circuit courts suggest that the type of data compromised should affect standing analysis.[186] These courts are correct that the type of data stolen affects the likelihood that a bad actor will misuse it.[187] Personal information varies and can include biometric data,[188] bank account numbers,[189] or home address

unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill."); *Remijas*, 794 F.3d at 696.

181. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 390 (6th Cir. 2016) (attributing questions of causation to "traceability" in the opinion, not to questions of if plaintiffs suffered an injury in fact).

182. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 642 (3d Cir. 2017) (Schwartz, J., concurring); *Remijas*, 794 F.3d at 696.

183. *Horizon*, 846 F.3d at 642.

184. FED. R. CIV. P. 56.

185. *E.g.*, Warth v. Seldin, 422 U.S. 490, 500 (1975) ("Although *standing in no way depends on the merits of the plaintiffs' contention that particular conduct is illegal*, it often turns on the nature and source of the claim alleged.") (emphasis added); Wilding v. DNC Servs. Corp., 941 F.3d 1116, 1128 (11th Cir. 2019) ("Whether a plaintiff has Article III standing is a question distinct from whether she has a statutory cause of action.").

186. *See, e.g.*, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 59 (D.C. Cir. 2019) (discussing "the nature of the information stolen" and "governmental character of the databases at issue"); In re SuperValu, Inc., 870 F.3d 763, 769 (8th Cir. 2017) ("We need not reconcile this out-of-circuit precedent [of data breach cases] because the cases ultimately turned on the substance of the allegations before each court.").

187. Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report* ¶ 2, FORBES (Aug. 14, 2019, 4:31 A.M.), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#6086b48e46c6 ("The issue with biometric data being stored in this way is that, unlike usernames and passwords, it cannot be changed. Once it's compromised, it's compromised. And for that reason this breach report will sound all kinds of alarms.").

188. *Office of Pers. Mgmt.*, 928 F.3d at 68 (addressing a data breach where fingerprints were exposed).

189. *E.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018).

information.[190] Stolen information may also be stale, or out of date, and thus less valuable to hackers.[191] But the type of data stolen should not affect whether plaintiffs have standing. The type of data compromised is a question of how much plaintiffs were harmed or whether the plaintiffs' mitigation costs were reasonable, not whether the plaintiffs have standing.[192]

2. Data Breaches as Breaches of Contract

Alternative to theories of harm grounded in tort law are those grounded in contract law, especially in jurisdictions that follow the economic-loss doctrine.[193] Under the economic-loss doctrine, courts may refuse to recognize economic losses under tort law when the parties have already chosen to order those same rights by express contract.[194] Indeed, many data breach plaintiffs bring causes of action under breach of contract,[195] of which there are three key formulations: (1) a plaintiff's *express* contract with the defendant to protect data,[196] (2) a plaintiff's *implied* contract with the defendant to protect data,[197] or (3) a plaintiff as a third-party beneficiary of an express contract between the defendant and another party, like a database vendor.[198] In each case, plaintiffs have standing as soon as they reasonably allege breach of a valid contract.

190. Lily Hay Newman, *supra* note 14, at ¶ 1.

191. *Data Breach*, MALWAREBYTES, https://www.malwarebytes.com/data-breach/ (last visited Dec. 9, 2019) (discussing how stolen data that is at least "two to three years old" is still valuable to hackers).

192. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 386 (2016) ("Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation.").

193. David Balser et al., *supra* note 7, at ¶ 18 ("It remains to be seen whether *Schnuck Markets* will gain traction outside the Seventh Circuit, but no court has rejected the Seventh Circuit's reasoning and one district court has relied on Schnuck Markets to dismiss financial institutions' claims.").

194. Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 812 (7th Cir. 2018) (quoting Indianapolis-Marion Cty. Pub. Library v. Charlier Clark & Linard, P.C., 929 N.E.2d 722, 729 (Ind. 2010)) ("The reason for this rule is that 'liability for purely economic loss . . . is more appropriately determined by commercial rather than tort law,' i.e., by the system of rights and remedies created by the parties themselves.").

195. *E.g.*, Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 616 (4th Cir. 2018); *In re* SuperValu, Inc., 870 F.3d 763, 771 n.6 (8th Cir. 2017); Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

196. *E.g.*, Kuhns v. Scottrade, Inc., 868 F.3d 711, 717 (8th Cir. 2017).

197. *SuperValu*, 870 F.3d at 767 (addressing a breach of implied contract claim).

198. Rottlund Homes of N.J., Inc. v. Saul, Ewing, Remick & Saul, L.L.P., 243 F. Supp. 2d 145, 153 (D. Del. 2003).

First, plaintiffs may allege that the targeted and compromised organization breached an express contract to "protect [plaintiffs'] sensitive information."[199] Plaintiffs who bring these claims essentially have automatic standing because a plaintiff who is a party to an express contract "has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged."[200] A stock brokerage, for example, may owe to its customers an express contractual obligation to "maintain sufficient security measures and procedures to prevent unauthorized access" to data.[201] Such a financial institution may also explicitly promise its customers that it will "use security measures," such as encryption, to "comply with federal law."[202] Plaintiffs still face a burden to allege that a defendant breached an express contractual provision; bare assertions that the defendant failed to protect data may prove insufficient.[203] However, assuming pleadings show that defendants breached an express contract, plaintiffs should simply have standing.

Second, plaintiffs have standing when they allege that a defendant organization breached an implied contract to take reasonable steps to protect data.[204] Certainly, a defendant may be at fault for a legal injury caused by a data breach if the defendant was contractually obligated to try to prevent the data breach.[205] Plaintiffs, however, may face a challenge convincing a court that an implied contract actually exists because an implied contract is "not formally or explicitly stated in words."[206] That is, the existence of an implied contract must be inferred from the parties' conduct given the facts and circumstances of a case, rather than referencing an explicit written agreement.[207]

199. Case v. Miami Beach Health Grp., Ltd., 166 F. Supp. 3d 1315, 1318–19 (S.D. Fla. 2016).

200. *SuperValu*, 870 F.3d at 771 n.6.

201. *Scottrade*, 868 F.3d at 717.

202. *Id.*

203. *See id.* (holding that plaintiffs merely alleged "bare assertions that Scottrade's efforts failed to protect customer [personally identifiable information]" and that "even if the security representations can be construed as promises of contract performance, the lengthy Consolidated Complaint fails to allege a specific breach of the express contract").

204. *SuperValu*, 870 F.3d at 771 n.6 (quoting Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016)) (internal quotations omitted).

205. Katz v. Pershing, LLC, 672 F.3d 64, 72 (1st Cir. 2012) ("From an analytical standpoint, we think . . . that when a plaintiff generally alleges the existence of a contract, express or implied, and a concomitant breach of that contract, her pleading adequately shows an injury to her rights.").

206. Dawes Min. Co. v. Callahan, 267 S.E.2d. 830, 831–32 (Ga. App. 1980), *aff'd* 272 S.E.2d 267 (Ga. 1980)).

207. *Id.;* Enslin v. The Coca-Cola Co., 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015).

These evidentiary differences make standing for the breach of an implied contract more difficult to demonstrate than for breach of an express contract. In *SuperValu*, for example, the Eighth Circuit found that the plaintiffs did not have standing because they failed to show that they were a party to an implied contract with a grocery store to "take reasonable steps to protect" data.[208] Although the *SuperValu* court did not rule out that the breach of an implied contract could ever be adequate for standing,[209] the court could have read the pleadings more leniently. Given the facts and circumstances, a better outcome would have been that the plaintiffs had standing. A reasonable grocery store customer "[o]rdinarily . . . does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access [transmitted] data," nor does a customer ever reasonably intend that their credit card information be provided to anyone but the merchant.[210] Undoubtedly, it would have been proper to conclude that the grocery stores had an implied contractual duty to "take reasonable measures to protect [customer] information."[211]

Moreover, the existence of an implied contract will be even less dubious if a defendant disseminates a privacy policy, regardless of whether the defendant is a brick and mortar business[212] or a website.[213] For example, the privacy policy on Yahoo's website has been held to constitute a contract to "employ reasonable safeguards" to protect users' personal information, despite Yahoo not specifically promising to invest time or money in cybersecurity.[214] Alternatively, a hotel chain's privacy policy that states the hotel is committed to safeguarding customer information may constitute an enforceable promise sufficient for standing.[215] Such a contractual duty may extend to guests for the period of time in which they stay on hotel premises.[216] Similarly, health care providers will likely be bound by implied contracts to protect

208. *SuperValu*, 870 F.3d at 771 n.6 (internal quotations omitted).

209. *See id.* ("Even if such analysis applies to an implied contract—a question we need not decide here—the complaint does not sufficiently allege that plaintiffs were party to such a contract.").

210. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011).

211. *Id.*

212. Walters v. Kimpton Hotel & Rest. Grp., LLC, 2017 WL 1398660, at *1–2 (N.D. Cal. Apr. 13, 2017).

213. *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., 2017 WL 3727318, at *48 (N.D. Cal. Aug. 30, 2017).

214. *Id.*

215. *Id.*

216. *Id.*

patients' data from thieves.[217] Health care providers may represent themselves as promising to protect personal information in their agreements with patients, website announcements, or press releases.[218] Then, patients agree to give up their sensitive personal information in exchange for the provider's "implicit and inescapable representation[]" that the health care provider will at least do "*something*" to protect patient information.[219] Plaintiffs may still not have standing if they allege the breach of an implied contract but without actual resulting injuries or damages.[220] And some courts do not consider the release of sensitive personal information without evidence of misuse to be an adequate injury.[221] But, as argued earlier in this Note, a data breach causes a cognizable legal injury both in terms of mental suffering[222] and actual financial loss incurred to purchase preventative services.[223]

Finally, under the third-party beneficiary doctrine, plaintiffs may have standing to sue for breach of contract even when they are not a party to the contract at issue. For example, a defendant in a data breach case may have entered into a contract with another company in which that company agreed to help the defendant protect its electronic business records. Those records may have included the plaintiffs' data with which the defendant was entrusted. In such a case, the defendant and the other company are co-stewards of the plaintiffs' information, and the plaintiffs are third-party beneficiaries of that contract.[224] Under the third-party beneficiary doctrine, plaintiffs in such a case need only show that there was a contract "made for the[ir] benefit . . . within the intent and contemplation of the contracting parties."[225] Essentially, "benefits flow to both the promisee and the third party, and either may sue to enforce the contract."[226] In a data breach case, a plaintiff might

217. Lozada v. Advocate Health & Diagnostic Corp., 2018 WL 7080045, at *6 (Ill. App. Ct. Dec. 24, 2018).

218. *Id.* at *2.

219. *Id.*

220. *E.g.*, Cherny v. Emigrant Bank, 604 F. Supp. 2d 605, 608 (S.D.N.Y. 2009).

221. *Id.*

222. *See supra* notes 142–156 and accompanying text.

223. *See supra* notes 172–178 and accompanying text.

224. *E.g.*, Mendez v. Hampton Court Nursing Ctr., LLC, 203 So. 3d 146, 148 (Fla. 2016); Flaherty & Collins, Inc. v. BBR-Vision I, L.P., 990 N.E.2d 958, 971 (Ind. Ct. App. 2013).

225. Rottlund Homes of N.J., Inc. v. Saul, Ewing, Remick & Saul, L.L.P., 243 F. Supp. 2d 145, 153 (D. Del. 2003).

226. *In re* Spong, 661 F.2d 6, 10 (2d Cir. 1981); *see also* Beckett v. Air Line Pilots Ass'n, 995 F.2d 280, 286 (D.C. Cir. 1993) ("[I]t is a fundamental principle of contract law that parties to a contract may create enforceable contract rights in a third party beneficiary."); RESTATEMENT (SECOND) OF CONTRACTS § 304 (1981) (illustrating the third-party beneficiary doctrine).

allege breach of an express provision requiring a database vendor to protect the compromised defendant's information.[227] Prior to the Capital One data breach discussed above,[228] where a hacker accessed over 100 million credit card numbers, Capital One had contracted with Amazon Web Services ("AWS") to store Capital One's data and software applications on cloud servers operated by AWS.[229] Potential liability following the Capital One data breach has not yet settled,[230] but the individual victims of the data breach could arguably sue to enforce the contract as third-party beneficiaries.[231] Each individual Capital One customer was a third-party beneficiary, with standing to sue for breach of contract, assuming the intent of the contract between Capital One and AWS was to protect customers' credit card data or it included a provision to the same effect.[232] It is worth noting that such contracts might validly prohibit third-party suits.[233] But whether a contract bans third-party beneficiary suits is a question of contract interpretation, not of whether a contract exists or if there is threshold standing.[234]

3. Federal Statutory Reinforcement

Common law considerations aside, plaintiffs in data breach cases may sue under federal statutory authority. And when a plaintiff sues under a federal statute, existence of a cognizable injury should be even

227. *E.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 73 (1st Cir. 2012).

228. *See supra* note 4 and accompanying text (discussing the Capital One data breach)

229. *Cloud Security at AWS is the Highest Priority*, AMAZON WEB SERVS. (2015), https://aws.amazon.com/campaigns/cloud-transformation/capital-one/.

230. *See* Kevin LaCroix, *Guest Post: Is Amazon Liable for the Capital One Hack?*, D&O DIARY (Aug. 19, 2019), https://www.dandodiary.com/2019/08/articles/cyber-liability/guest-post-is-amazon-liable-for-the-capital-one-hack/ (suggesting that AWS could be liable for the Capital One data breach and stating that "just about every corporate data breach that involves a third party vendor results in some level of finger-pointing between the two").

231. *See id.* at "The AWS/Capital One Contract" (restating provisions of the contract between Capital One and AWS and concluding that "[t]he above provisions are not ambiguous, and clearly define data security responsibilities to belong to the AWS customer").

232. *Id.*

233. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 2011 WL 1232352, at *1, *18 (S.D. Tex. Mar. 31, 2011); Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 324 (M.D. Pa. 2005) ("While [The Restatement, adopted here by the state] recognizes that a nonsignatory to a contract can be an intended beneficiary of the contract if certain conditions are met, it recognizes the right of the contracting parties to exclude third parties from invoking the benefits of their agreement."); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 302 (1981).

234. *See* Katz v. Pershing, LLC, 672 F.3d 64, 72–73 (1st Cir. 2012); *Heartland Payment Sys.*, 2011 WL 1232352, at *16–18 (discussing third-party suits in the context of Rule 12(b)(6)).

less dubious than if it were under common law.[235] Sometimes, a statute provides plaintiffs a cause of action by simply elevating the legal status of a common law harm.[236] Or, Congress may enact a statute to "give rise to a case or controversy where none existed before."[237] In either case, federal statutes introduce to standing analysis rights that Congress deliberately sought to protect.[238] For example, the disclosure of personal information became a de facto injury when Congress enacted FCRA.[239] Labeling an event like a data breach as a de facto injury may appear to ignore the requirement that an injury be "actual or imminent," essentially collapsing analysis to only address the "particularized" and "concrete" requirements. But there is no need to address imminence of future harm alleged in such a case because the loss of privacy caused by a data breach is an actual and present injury.[240]

To be sure, Congress could enact legislation that specifically creates a private right of action for data breach victims, as suggested by many commentators.[241] This Note does not address the intricacies or political practicality of such a federal statute, other than agreeing that such an enactment is a good idea. A federal statute aimed at broadly providing data breach victims with a cause of action would likely eliminate many challenges plaintiffs face in satisfying standing requirements.[242] Such a statute would also advance the public policies later outlined in Part IV of this Note.[243]

---

235. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639–40 (3d Cir. 2017) (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)) ("[S]ince the 'intangible harm' that FCRA seeks to remedy 'has a close relationship to a harm [i.e. invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,' we have no trouble concluding that Congress properly defined an injury that 'give[s] rise to a case or controversy where none existed before.'").

236. Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992).

237. *Spokeo*, 136 S. Ct. at 1549 (quoting *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring)).

238. *E.g.*, *id.*; *Horizon*, 846 F.3d at 634.

239. *Horizon*, 846 F.3d at 639 ("[W]ith the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm.").

240. *Id.* at 641 (Schwartz, J., concurring) ("Plaintiffs allege[d] that the theft of the laptops caused a loss of privacy, which is itself an injury in fact.").

241. *E.g.*, Michael Hopkins, *Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches*, 50 U. PAC. L. REV. 427, 445–46 (2019); Lorio, *supra* note 23, at 127.

242. Lorio, *supra* note 23, at 127–28.

243. Relatedly, bailment of intangible property may be a promising theory of harm. However, courts to date barely address data bailment, other than nothing that "[i]n certain circumstances, intangible property may be the subject of a bailment." Richardson v. DSW, Inc., 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005); *see also* Weitz & Luxenberg, *Bailment Claims: A Cause of Action In Data Breach Cases*, WIETZ & LUXENBERG BLOG (Apr. 14, 2015),

B. Courts Misunderstand Clapper*'s Application to Data Breach Lawsuits*

Because of the above delineations of legal harm, *Clapper*'s requirement that plaintiffs show that future harm is "imminent" should not apply to data breach lawsuits; *Clapper*'s facts and those of data breach cases markedly differ. A data breach is generally a past and confirmed event, with victims' personal information exposed or acquired.[244] On the other hand, *Clapper* involved allegations of potential wiretapping by the federal government, which was a speculative future occurrence.[245] Further, the plaintiffs' claims in *Clapper* were based exclusively on those future wiretapping claims occurring.[246] However, none of the plaintiffs had been wiretapped, nor did any of them have knowledge that the government would ever wiretap them.[247] Rather, the plaintiffs' allegations were based on a series of assumptions and contingencies.[248] The plaintiffs alleged (1) that the government planned to imminently target their communications;[249] (2) that the government's choice to target the plaintiffs' communications was pursuant to the Foreign Intelligence Surveillance Act, as opposed to a different federal power;[250] and (3) that after the government targeted the plaintiffs' communications, a separate set of decisionmakers would then actually authorize the surveillance.[251] The Court refused to find that the plaintiffs had standing because they had merely alleged a "chain of possibilities"

---

https://www.weitzlux.com/blog/2015/04/14/bailment-claims-cause-action-data-breach-cases/ (discussing a lack of data bailment cases). Even in such a case, plaintiffs still need to allege the elements of traditional bailment. *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) ("Plaintiffs are correct that intangible property such as their personal financial information can constitute property subject to bailment principles, they have not—and cannot—allege that they and Target agreed that Target would return the property to them."). If data bailment claims' validity as legitimate claims on the merits are unclear, then so are questions of standing.

244. Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

245. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410–11 (2013).

246. *Id.* at 402.

247. *Id.* at 411.

248. *Id*.

249. *Id.*

250. *Id.* at 412. Additionally, whether the government surveilled the plaintiffs pursuant to Section 702 of the Foreign Intelligence Act was a question of traceability, not just of whether there was an injury in fact. *Id.* at 410–11. That is, the plaintiffs had to show that their alleged injuries were fairly traceable to the government acting under that specific statute. The plaintiffs failed to show such traceability. *Id.*

251. *Id.* at 413.

requiring "guesswork as to how independent decisionmakers will exercise their judgment."[252]

A data breach lawsuit is far removed from those facts because the unauthorized exposure of data already has already occurred; it is not a speculative or assumed future occurrence.[253] Additionally, any subsequent future harm caused by a data breach, like identity theft or fraud, stems from and is closely attached to that previous data breach.[254] These distinguishing facts alone limit *Clapper*'s applicability. Accordingly, *Clapper*'s requirement that injuries be "certainly impending" should not control standing for data breach suits. Instead, courts should, at a minimum, use the lower standard of "substantial risk" of future harm or, with sufficient facts alleged, use neither and find that an "actual" injury occurred.

Some circuit courts properly recognize this distinction. The Seventh Circuit in *Remijas* noted that in *Clapper* "there was no evidence that any of the [plaintiff]s' communications either had been or would be monitored."[255] But in a data breach case, there is "no need to speculate" because information has already been stolen.[256] The Ninth Circuit similarly in *Zappos* stated that a laptop thief has "all the information he need[s] to open accounts or spend money in the plaintiffs' names."[257] In contrast, identifying harm in *Clapper* had required a "speculative multi-link chain of inferences."[258] *Clapper* provides guidance for analyzing standing but should by no means be used to force imminence analysis into data breach cases.

C. By Treating Data Breaches as Inherently Injurious, Courts Do Not Risk Undermining Standing's Role as a Separation of Powers Doctrine

Standing is grounded in separation of powers principles, ensuring that courts rule on only "cases" and "controversies," rather than

252. *Id.* at 413–14.

253. *E.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017) ("Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill."); Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 692–93 (7th Cir. 2015).

254. *Attias*, 865 F.3d at 628.

255. *Remijas*, 794 F.3d at 693 (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).

256. *Id.* (quoting *Adobe*, 66 F. Supp. 3d at 1214).

257. *In re* Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018).

258. *Id.*

creating de facto legislation by ruling on hypothetical situations.[259] A data breach and its fallout are not such hypothetical situations. In a data breach lawsuit, plaintiffs sue to redress their private legal rights over an event that has already occurred. It is possible that after a case on the merits a defendant organization may not be at fault, but to make those determinations, courts must allow data breach cases to proceed. Besides, hackers obtain information with the intent to misuse it.[260] Whether the breached organization is at fault for that misuse not a question of standing.[261] By finding that data breach plaintiffs have standing, courts do not risk usurping the power of the legislative or executive branches.[262]

IV. POLICY CONSIDERATIONS

There are several policy considerations weighing in favor of finding that data breach plaintiffs have standing in addition from the above legal analysis. Concluding that a data breach is harmful in and of itself makes good practical sense.

A. The "Wait and See" Approach Unnecessarily Harms Both Consumers & Companies

Harm need not have already occurred or be "literally certain" to constitute an injury in fact.[263] Likewise, every data breach victim need not have already suffered actual identity theft or fraud to suffer a legally cognizable injury.[264] Such a policy benefits plaintiffs by allowing them to redress their injuries quickly so that future or ongoing harm is minimized.[265] A similar principle applies to why courts grant preliminary injunctions.[266] As soon as a victim's information is exposed,

259. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401, 408 (2013).

260. *Remijas*, 794 F.3d at 693.

261. *Zappos*, 888 F.3d at 1029.

262. Joslin, *supra* note 19, at 754 ("Data breach litigation typically takes the form of private individuals suing to redress their own private rights. In this context, there is no threat of judicial entanglement in political disputes, nor is there concern about the judiciary usurping political powers.").

263. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (quoting *Clapper*, 568 U.S. at 414 n.5).

264. *Id.*

265. Univ. of Tex. v. Camenisch, 451 U.S. 390, 395 (1981) ("The purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be held. . . . A party thus is not required to prove his case in full at a preliminary-injunction hearing.").

266. *See* Jeffrey M. Sanchez, *The Irreparably Harmed Presumption? Why the Presumption of Irreparable Harm In Trademark Law Will Survive eBay And Winter*, 2011 B.Y.U. L. REV. 535,

that victim has already suffered an injury in fact. And each day that victim any other victim must wait to seek redress, they will suffer even more harm in the form of looming or ongoing misuse of their data.[267] In some cases, a portion of plaintiffs have already experienced fraud by the time they sue, with others expecting data misuse "sooner or later."[268] From a policy standpoint, customers "should not have to wait until hackers commit identity theft or credit-card fraud in order to [have] standing."[269]

When plaintiffs ultimately bring suit is a difficult decision. Proving and winning large money damages may be easier if plaintiffs wait to sue after a data breach, allowing for more harm to definitively materialize.[270] Meanwhile, the more time that passes between a data breach and litigation, the more latitude a defendant has to argue a lack of causation.[271] Either way, a plaintiff's decision of when to sue should not be made for them by an improper conception of Article III standing.

Companies may also benefit from earlier data breach lawsuits because they value certainty in both financial burdens[272] and legal liability.[273] If a lawsuit is inevitable, a breached organization, in addition

535 (2011) ("[A] preliminary injunction serves to 'stop the bleeding' early on in litigation and can mitigate potential damage to the trademark owner's reputation."); Jim Barr Coleman, *Digital Photography and the Internet, Rethinking Privacy Law*, 13 J. INTELL. PROP. L. 205, 214 (2005) ("Traditionally, the purpose of a preliminary injunction is that you stop the bleeding.").

267. Remijas v. Nieman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737: REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007)), https://www.gao.gov/new.items/d07737.pdf) ("Further, once stolen data have been sold or posted on the Web, fraudulent use of that information my continue for years.").

268. *Id.* at 693–94.

269. *Id.* at 693.

270. *Id.*

271. *Id.* (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)).

272. *See, e.g.*, Will Kenton, *Certainty Equivalent Definition*, INVESTOPEDIA, https://www.investopedia.com/terms/c/certaintyequivalent.asp (last updated Apr. 21, 2019) ("Investments must pay a risk premium to compensate investors for the possibility that they may not get their money back and the higher the risk, the higher premium an investor expects over the average return. . . . A company seeking investors can use the certainty equivalent as a basis for determining how much more it needs to pay to convince investors to consider the riskier option.").

273. *See, e.g.*, John R. Allison, *Five Ways to Keep Disputes Out of Court* ¶ 1, HARV. BUS. REV. (Feb. 1990), https://hbr.org/1990/01/five-ways-to-keep-disputes-out-of-court ("[T]here are few things managers dread more than litigation. Even petty cases have a way of damaging relationships, tarnishing reputations, and eating up enormous sums of money, time, and talent."); Thomas H. Belknap Jr., *Calculating Settlement Value of a Case* ¶ 1, BLANK ROME LLP (Apr. 2014), https://www.blankrome.com/publications/calculating-settlement-value-case-0.

to trying to avoid substantial monetary liability, may want to resolve the lawsuit as soon as possible.[274] For that reason in particular, companies may value forcing plaintiffs into arbitration.[275] Or if arbitration is not possible, companies may prefer federal class actions because they can resolve every claim in a single action, even when the litigation presents a risk of sweeping adverse outcomes.[276] By no means do all companies necessarily agree. "For corporate interests, class actions are often viewed as a two-edged sword, offering enormous risks and tremendous opportunities to resolve outstanding litigation issues in one fell swoop."[277] But denying standing to data breach plaintiffs prevents this route altogether by forcing plaintiffs to postpone lawsuits, leaving companies guessing as to when they will finally be served.

B. Federal Class Actions Are More Efficient Than State Suits

Granting standing to plaintiffs in data breach cases will not burden companies with lawsuits any more than they otherwise would face. Even if plaintiffs had immense difficulty proving standing, they would likely still bring federal suits, just later, once more harm materialized. Although plaintiffs can always bring data breach suits in state courts, where the plaintiffs would likely more easily have standing,[278] it seems likely that plaintiffs would continue in federal courts. In federal courts, plaintiffs may take advantage of the plaintiff-friendly Class Action Fairness Act ("CAFA"),[279] multi-district litigation ("MDL") that allows plaintiffs to consolidate cases nationally,[280] and federal statutes like FCRA. Moreover, plaintiffs in federal court can still bring state law

274. *See* David Rosenberg, *Mass Tort Class Actions: What Defendants Have and Plaintiffs Don't*, 37 HARV. J. ON LEGIS. 393, 430 (2000) ("[D]efendant firms are structured to operate risk neutrally and have many means of hedging against risk, notably derived from laws limiting liability and affording protection in bankruptcy, opportunities for stockholders to diversify their portfolios, and widespread availability of liability insurance.").

275. *See* Jessica Silver-Greenberg & Robert Gebeloff, *Arbitration Everywhere, Stacking the Deck of Justice* ¶¶ 1–3, N.Y. TIMES (Oc. 21, 2015), https://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html (discussing arbitration clauses as a method for companies to circumvent the court system).

276. James M. Underwood, *Rationality, Multiplicity & Legitimacy: Federalization of the Interstate Class Action*, 46 S. TEX. L. REV. 391, 403 (2004).

277. *Id.*

278. Willis, *supra* note 158, at 253–54 (citing state court cases from Michigan, Alaska, California, New Jersey).

279. Class Action Fairness Act of 2005 ("CAFA"), Pub. L. 109-2 (2005).

280. 28 U.S.C. § 1407 (2018) (laying out "multidistrict litigation" standards).

claims, like the powerful California Consumer Privacy Act ("CCPA")[281] under diversity jurisdiction.[282]

Finding that data breach plaintiffs have standing will also be unlikely to increase companies' litigation burdens because the many tools at federal courts' disposal increase judicial efficiency. Through economies of scale in class action suits, defendants can amalgamate evidence; and plaintiffs no longer need to bring scattered and distinct state suits.[283] Although state court systems wield their own class action statutes,[284] federal courts are likely more efficient for plaintiffs and defendants alike to adjudicate national data breach incidents.

C. Consumers as "Private Attorneys General" Help Create Proper Corporate Cybersecurity

The more likely it is that a company will face legal liability following a data breach, the more incentivized that company will be to adopt robust cybersecurity practices.[285] Finding that plaintiffs have standing in data breach cases will increase the ease at which victims can bring suits, and companies will in turn invest in privacy infrastructure to deter and prevent would-be hackers.[286] Companies already have compelling

281. Cal. Civ. Code § 1798.100 (West 2020).

282. 28 U.S.C. § 1332(a) (2018).

283. *See* David Rosenberg, *supra* note 274, at 394 ("With class-wide aggregation of the defense interest, the defendant exploits economies of scale to invest far more cost-effectively in preparing its side of the case than plaintiffs can in preparing their side.").

284. *E.g.*, Fla. R. Civ. P. 1.220 (1993).

285. Although deterrence is often discussed in terms of how damages should be calculated and imposed, the deterrent effects of more permissively letting suits proceed with standing should have a similar effect, as if damages for civil liability were increased. *See* John C. Manning, *Going Back to Scrap in Order to Refine Steel: The Supreme Court Loosens the Modern Constraints on the Doctrine of Standing in* Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 10 WIDENER J. PUB. L. 215, 230–31 (2001) (discussing that "an award of civil penalties . . . would prevent the defendant's conduct through deterrence"); Timothy Stoltzfus Jost & Sharon L. Davies, *The Empire Strikes Back: A Critique of the Backlash Against Fraud and Abuse Enforcement*, 51 ALA. L. REV. 239, 266 (1999) ("In tort cases, it has been argued that damages should normally be calibrated to achieve what is referred to as 'optimal deterrence,' i.e., damages should be set sufficiently high to ensure that a tortfeasor fully internalizes all the costs that her conduct imposes on a victim . . . .").

286. The idea of deterrence through threat of liability is exemplified in antitrust law, in which the Clayton Act, 15 U.S.C. § 15(a) (2018), allows private plaintiffs to collect treble damages, thereby incentivizing private citizens to zealously sue companies for antitrust violations. *See* Ill. Brick Co. v. Illinois, 431 U.S. 720, 745–46 (1977) (discussing the legislative intent behind treble damages to be enforcement by "private attorneys general"); Hanover Shoe, Inc. v. United Shoe Mach. Corp., 392 U.S. 481, 484 (1968) ("Treble-damage actions, the importance of which the Court has many times emphasized . . . ."); Jason Wasserman, Apple v. Pepper*: Applying the Indirect Purchaser Rule to Online Platforms*, 14 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 147, 153 (2019) (quoting *Illinois Brick*, 431 U.S. at 746) ("In large part, the rule was created to

reasons to protect their data. Data breach litigation costs companies millions of dollars in legal expenses, computer system rehabilitation costs, and bad press.[287] But finding that plaintiffs have standing will provide an even greater incentive to improve cybersecurity practices without coercion.[288] Compromised organizations, often corporations, are also least-cost avoiders[289] for improving privacy infrastructure in the United States. If and when companies do ultimately adopt strong cybersecurity practices, the companies should in theory be compromised less often.

CONCLUSION

Cyberattacks and subsequent data breaches increase every year, depriving individuals control of their personal information. Whether it is the breached company's fault, or solely the fault of the hacker, depends on the merits of each case, and plaintiffs should be able to bring lawsuits against breached organizations swiftly and reliably to resolve those questions. Some courts, however, have wrongly found that data breach victims do not have standing because the future harm caused by a data breach is too "speculative." But the exposure of information from a data breach is an injury in and of itself. Courts should find that victims of data breaches suffer injuries in fact sufficient for standing the moment that their information is disclosed without their consent. Doing so will reinforce common law rights, efficiently resolve liability, and better protect consumers.

---

incentivize private antitrust actions by direct purchasers, or so-called 'private attorneys general.'").

287. *What's the Real Cost of a Data Breach?*, PKWARE BLOG, https://www.pkware.com/blog/what-s-the-real-cost-of-a-data-breach (last updated Sept. 2019).

288. *See* Air & Liquid Sys. Corp. v. DeVries, 139 S. Ct. 986, 997 n.3 (2019) (Gorsuch, J., dissenting) (quoting Nat'l Union Fire Ins. Co. of Pittsburgh v. Riggs Nat'l Bank of Washington, D.C., 5. F.3d 554, 557 (D.C. Cir. 1993)) ("'Placing liability with the least-cost avoider increases the incentive for that party to adopt preventive measures' that will 'have the greatest marginal effect on preventing the loss.'").

289. *See* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused By Hacked Devices?*, 50 U. MICH. J.L. REFORM 913, 916 (2017) ("[H]olding manufacturers liable for downstream harms caused by their insecure devices is well aligned with the purposes of products liability law—to minimize harm by encouraging manufacturers (*as a least-cost-avoider*) to invest in security measures." (emphasis added)); Guido Calabresi, *Civil Recourse Theory's Reductionism*, 88 IND. L.J. 449, 456–57 (2013) (discussing how the "first party" in an accident is often the "least-cost-avoider/best decider").