Minnesota Journal of Law, Science & Technology

Volume 17 | Issue 2 Article 9

6-2016

It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation

John Biglow

Note

It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation

*John Biglow**

According to a recent study by the Identity Theft Resource Center,[1] 781 data breaches occurred in the United States in 2015.[2] Although the size of these breaches differ, the number of Americans affected is in the hundreds of millions.[3] Being the victim of a data breach typically carries with it the threat of fraudulent charges or identity theft; however, plaintiffs alleging these harms have faced a common roadblock in litigation.[4] In order for a plaintiff to have standing according to Article III

---

* JD candidate, 2017, University of Minnesota Law School. I would like to thank Professors Thomas Cotter and William McGeveran for their insight and feedback, as well as the MJLST editors and staff, specifically James Meinert and Mickey Stevens. I would also like to thank my friends and family for all of their encouragement throughout this process, specifically Chloë Cardinal for her patience, understanding, and encouragement.

1. The Identity Theft Resource Center is a United States based nonprofit which focuses on providing free assistance to identity theft victims. *See* IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/ (last visited Feb. 20, 2016).

2. *See Identity Theft Resource Center Breach Report its Near Record High in 2015*, IDENTITY THEFT RES. CTR. (Jan. 25, 2016), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html [hereinafter *Identity Theft*].

3. *See generally* IDENTITY THEFT RES. CTR., DATA BREACH REPORTS (2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf (reporting the details of 2015 data breaches including the number of people affected). The number of records breached in the healthcare sector alone numbered over 112 million in 2015. *See* Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records in* 2015, FORBES (Dec. 31, 2015, 9:11 PM), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#416631f67fd5.

4. *See* Dana Post, *Plaintiffs Alleging Only "Future Harm" Following a Data Breach Continue to Face a High Bar*, INT'L ASS'N PRIVACY PROFESSIONALS (Jan. 28, 2014), https://iapp.org/news/a/plaintiffs-alleging-only-future-harm-following-a-data-breach-continue-to-fa.

of the United States Constitution, a plaintiff must have suffered an injury that is "concrete, particularized, and actual or imminent."[5] In recent years, many courts have been unwilling to grant Article III standing to data breach plaintiffs, ruling for one reason or another that the "harm" the plaintiffs claim to have suffered cannot be shown to be either actual or imminent.[6] Federal circuit courts are split on the issue of whether plaintiffs can satisfy Article III's standing requirement while alleging only future harm or harm based on prophylactic measures taken to protect against future harm; the Ninth and Seventh Circuits have allowed standing in these cases while the Third Circuit has refused standing.[7] When the United States Supreme Court decided *Clapper v. Amnesty International USA* in 2013, a case which concerned the requirements for Article III standing,[8] many posited that *Clapper* may foreclose plaintiffs from successfully establishing standing based on future harm in data breach cases.[9] In 2015, the Seventh Circuit decided in *Remijas v. Neiman Marcus Group, LLC* that *Clapper* does not foreclose Article III standing based on allegations of future harm and the taking of prophylactic measures to pre-

5. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).

6. *E.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (holding that allegations of possible future injury stemming from a data breach were not sufficient to satisfy Article III standing because the threatened injury was not certainly impending); Amanda Fitzsimmons et al., *Seventh Circuit: Victims of Data Breaches Have Article II Standing to Litigate Class Action Lawsuits*, DLA PIPER (July 23, 2015), https://www.dlapiper.com/en/us/insights/publications/2015/07/seventh-circuit-victims-of-data-breaches/ ("To date, an overwhelming majority of courts have dismissed data breach consumer class actions at the outset due to a lack of cognizable injury-in-fact, an essential element for standing under Article III of the US Constitution.").

7. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased future risk of identity theft resulting from a stolen laptop containing names, addresses and social security numbers of 97,000 employees was sufficient to establish Article III standing), *and* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that an increased future risk of harm is sufficient to confer Article III standing), *with Reilly*, 664 F.3d at 42 (holding that allegations of possible future injury stemming from a data breach were not sufficient to satisfy Article III standing because the threatened injury was not certainly impending).

8. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

9. *Does Clapper Silence Data Breach Litigation? A Two-Year Retrospective*, INFOLAWGROUP (Feb. 25, 2015), http://www.infolawgroup.com/2015/02/articles/breach-notice/does-clapper-silence-data-breach-litigation-a-two-year-retrospective/ (arguing that *Clapper* has made it highly unlikely for plaintiffs to establish standing in cases alleging a risk of future harm).

vent this harm when the harm is imminent; this signaled to the legal world that the circuit split had survived *Clapper*.[10]

This Note will argue that the threat of future harm in data breach cases, and the prophylactic measures taken to protect against this future harm, should satisfy the injury-in-fact requirement of Article III and establish standing. Furthermore, it will argue that ultimately, if the opportunity arises, the United States Supreme Court should resolve the current circuit split and adopt a ruling similar to that of the *Remijas* court. Part I of this Note discusses how state and federal statutes and the federal circuits have attempted to address the issue of Article III standing based on allegations of future harm in data breach cases. Part I begins with a brief introduction on data breaches and the resulting litigation. Next, Section I.B. discusses Article III's standing requirements and how federal case law has interpreted its requirements in the data breach context. Section I.C. briefly discusses the potential relevance of *Spokeo, Inc. v. Robins*, a case currently in front of the United States Supreme Court, to this issue.[11] Finally, Sections I.D and I.E. briefly look at how state and federal statutory law has sought to curtail the data breach problem by introducing various notification statutes. Part II of this Note will analyze, critique, and compare the body of law discussed in Part I. Part II begins with an analysis of the federal case law, including the circuit split, and the relevance of *Clapper* and *Spokeo, Inc.* to this issue. Section II.C. concludes with a proposal that, depending on how the Court comes out in the *Spokeo, Inc.* case, the Court, if the opportunity arises, should ultimately resolve the existing circuit split in favor of a ruling in line with the *Remijas* court's reasoning.

---

10. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding that allegations of future harm and mitigation expenses can establish Article III standing when the harm is imminent and reasoning that the harm is imminent in data breach cases since the hackers presumably conducted the data breach to make fraudulent charges or assume the identities of those whose data was breached); Kristin Shepard, *Data Breach Class Claims Survive* Clapper, A.B.A. (Sept. 9, 2015), http://apps.americanbar.org/litigation/committees/classactions/articles/summer2015-0915-data-breach-class-claims-survive-clapper.html.

11. *See* Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014), *cert. granted*, 135 S. Ct. 1892 (U.S. Apr. 27, 2015) (No. 13-1339).

I. BACKGROUND

A. DATA BREACHES AND THE RESULTING LITIGATION

Most modern companies ask their customers and employees for their personal information, whether it be financial, like a credit card number, or identification based, like an address or a social security number.[12] According to the Federal Trade Commission (FTC), many of these companies store this information either "in their files or on their network."[13] A data breach occurs whenever this stored information is accessed by an unauthorized third party. Since the mid 2000's, data breaches have become quite common.[14] According to Privacy Rights Clearinghouse, a U.S. based nonprofit which specializes in consumer privacy rights, advocacy, and education, and has recorded U.S. data breach records since 2005, there have been 4789 breaches which have been made public since 2005, with 896,258,345 records being compromised.[15] This number of records seems high until one realizes that many of the larger breaches involved tens of millions of accounts, with some, notably the Target Corporation breach of 2013 and the eBay Inc. breach of 2014, potentially involving over one hundred million accounts each.[16]

---

12. *See, e.g.*, *Start with Security: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Mar. 13, 2016).

13. *Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Feb. 28, 2016).

14. *See Chronology of Data Breaches: Security Breaches 2005 – Present*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breach/new [https://perma.cc/4KQL-CRRH].

15. *Id*.

16. *See* Lorenzo Ligato, *The 9 Biggest Data Breaches of All Time*, HUFFINGTON POST (Aug. 21, 2015), http://www.huffingtonpost.com/entry/biggest-worst-data-breaches-hacks_us_55d4b5a5e4b07addcb44fd9e (listing the nine largest U.S. data breaches, measuring from 56 million (The Home Depot, Inc., 2014), to 160 million (various American businesses, 2005–2012)); Chris Isidore, *Target: Hacking Hit up to 110 Million Customers*, CNN MONEY (Jan. 11, 2014, 6:20 PM), http://money.cnn.com/2014/01/10/news/companies/target-hacking/ (reporting that the Target Corporation breach affected as many as 40 million customers' credit or debit card information and as many as 70 million customers' personal information, "such as their name, address, phone number and email[s]" were hacked); Andrea Peterson, *eBay Asks 145 Million Users to Change Passwords After Data Breach*, WASH. POST (May 21, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/ (reporting that the

When a company suffers a data security breach in which their customers' or employees' personal information is stolen or accessed, legal claims by the affected customers or employees often follow.[17] Allegations commonly claim either a breach of a legal duty by the company due to lax security or that the plaintiffs have suffered some sort of "recoverable injury;"[18] this Note concerns the latter group of claims. Data breach cases in which plaintiffs claim to have suffered a recoverable injury are commonly divided into two categories.[19] In the first category are individuals whose information has been stolen and utilized by the thief for financial gain.[20] These individuals face the least amount of roadblocks in litigation,[21] and due to this, this category will not be discussed in this Note. The second category includes individuals whose information has been stolen or accessed in a data breach but who have not yet suffered any financial loss stemming from the unauthorized use of their information.[22] These individuals allege to have suffered an injury

---

eBay breach occurred "between late February and early March" of 2014, that the hackers gained access to "encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth," and that although eBay did not report how many of its accounts had been breached, it nonetheless asked all 145 million of its users to change their passwords as a precautionary measure).

17. *See* Douglas H. Meal & David T. Cohen, *Private Data Security Breach Litigation in the United States*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES 101, 102 (2014) ("Although data security breaches are now commonplace, those breaches where personal information is stolen or put at risk of being stolen often trigger legal claims by private plaintiffs seeking to characterize the breach as the result of unreasonable, lax measures by the breached company in protecting the personal information in question . . . . [S]uch plaintiffs frequently struggle to plead and prove that the data security breach resulted from the victim's breach of its legal obligations, as opposed to an unfortunate perpetration of computer crime by third parties, and/or that any breach of legal obligations caused any recoverable injury." (footnote omitted)).

18. *Id*.

19. *See, e.g.*, Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 398–99, 404 (2014) (listing two classes of cases after a data breach has occurred; Class I cases in which the plaintiff has suffered a financial loss stemming from a data breach and Class II cases in which the plaintiff has taken steps to prevent future harm stemming from a data breach or they have alleged that future harm is imminent due to a data breach).

20. In the first class of cases, the plaintiffs personal or financial information has been stolen by a third party, and that third party has used that information to make purchases using the plaintiffs' money. *See id*. at 398–99.

21. *See id*. at 399; Post, *supra* note 4.

22. *See* Cease, *supra* note 19, at 399 ("The second class of cases—Class II Cases—are those in which the plaintiffs' information has been accessed but

based upon the threat that they may suffer a loss in the future, or that they have suffered an injury in taking steps to protect themselves from this future loss; it is common for plaintiffs to allege both.[23] Plaintiffs that find themselves in this second category face significant challenges in litigation.[24] This second category of cases will form the main scope of this Note.

B. ARTICLE III STANDING REQUIREMENT AND ITS INTERPRETATION IN FEDERAL DATA BREACH CASES

In order for a federal court to have the jurisdiction to hear a case, it must satisfy Article III's "cases or controversies" requirement.[25] Part of this requirement is that plaintiffs "must establish that they have standing to sue," at the pleading stage.[26] In order to have standing, a plaintiff must have an "injury-in-fact, which is an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical."[27] In order for a pending future injury to be "imminent," it must be "certainly impending."[28] The United States Supreme Court has not uniformly required a showing that a future injury is "literally certain," and has allowed standing in some cases where there is a "'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that

---

that information has not been used to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiffs. However, these plaintiffs typically claim that they have been harmed in other ways: incurring costs for credit-monitoring services, paying the costs of cancelling and receiving new bank cards, suffering loss of reward points from cancelled cards, and enduring general anxiety that their information will be used in the future to make unauthorized purchases.").

23. *See id.* In this Note these types of alleged injuries will be classified as "the threat of future harm," and "the prophylactic measures taken to protect against this future harm."

24. *See generally* Post, *supra* note 4 (discussing outcomes in cases filed over future harms from a data breach).

25. *See* U.S. CONST. art. III, § 2; Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011) ("Article III limits our jurisdiction to actual 'cases or controversies.'").

26. *Reilly*, 664 F.3d at 41 ("One element of this 'bedrock requirement' is that plaintiffs 'must establish that they have standing to sue.'" (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997))).

27. *Id.* at 41–42 (quoting Danvers Motor Co. v. Ford Motor Co., 432 F.3d 286, 290–91 (3d Cir. 2005)).

28. *Id.* at 42 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

harm."[29] Circuit courts have split over the issue of whether the threat of future harm stemming from a data breach and the prophylactic measures taken to protect against this future harm satisfy this Article III standing requirement.[30]

1. *Pisciotta*, *Krottner*, and *Reilly*; the Circuit Split Begins

When the Seventh Circuit decided *Pisciotta v. Old National Bancorp* in 2007, it became the first of the circuit courts to address the issue of Article III standing for allegations of future harm and the prophylactic measures taken to protect against this harm in the data breach context.[31] The plaintiffs in the case were Luciano Pisciotta and Daniel Mills, who brought the action on behalf of a class of individuals who had provided information to Old National Bancorp (ONB) either as customers or potential customers.[32] ONB had suffered a security breach in which these class members' personal and financial information had been accessed.[33] Significantly to the issue of standing, the plaintiffs did not allege in their complaint any "*completed direct* financial loss to their accounts as a result of the breach," but instead alleged they had "incurred expenses in order to prevent their confidential personal information from being used and will continue to incur expenses in the future."[34] The court decided in favor of conferring Article III standing, reasoning that, "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[35]

---

29. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) (citing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–55 (2010)).

30. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased future risk of identity theft resulting from a stolen laptop containing names, addresses and social security numbers of 97,000 employees was sufficient to establish Article III standing), *and* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that an increased future risk of harm is sufficient to confer Article III standing), *with Reilly*, 664 F.3d at 42 (holding that allegations of possible future injury stemming from a data breach were not sufficient to satisfy Article III standing because the threatened injury was not certainly impending).

31. *See Pisciotta*, 499 F.3d at 634.

32. *Id*. at 631–32.

33. *Id*. at 632.

34. *Id*.

35. *Id*. at 634.

The *Pisciotta* court supported its reasoning by stating that it was in line with "many of [their] sister circuits."[36] In a footnote, the court cited four cases as persuasive precedent: *Denney v. Deutsche Bank AG*, *Sutton v. St. Jude Medical S.C., Inc.*, *Central Delta Water Agency v. United States*, and *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*[37] Though the Pisciotta court considered these future harm cases to be persuasive and instructive, they provided little analysis for why these fact patterns are analogous or why the analogies are apt. In *Denney*, the plaintiffs alleged fraudulent and improper tax counseling.[38] The *Pisciotta* court cited dicta from *Denney* in which they discuss how, "exposure to toxic or harmful substances . . . [can] satisfy the Article III injury-in-fact requirement even without physical symptoms of injury caused by the exposure."[39] In *Sutton,* the court held that Article III standing was present based on the increased risk of future harm stemming from a defective medical device.[40] In *Central Delta*, the court conferred standing to a group of farmers who claimed a risk of future harm to their crops if the United States Bureau of Reclamation's plans increased the salinity of available irrigation water.[41] In *Friends of the Earth*, the court found stand-

---

36. *Id*. at 634.

37. *Id*. 634 n.3; Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (discussing, in dicta, injury based on exposure to toxic substances); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (concerning defective medical devices); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (concerning environmental harm); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (en banc) (concerning environmental harm).

38. *See Denney*, 443 F.3d at 253.

39. *Id*. at 264–65 ("For example, exposure to toxic or harmful substances has been held sufficient to satisfy the Article III injury-in-fact requirement even without physical symptoms of injury caused by the exposure, and even though exposure alone may not provide sufficient ground for a claim under state tort law.").

40. *See Sutton*, 419 F.3d at 574–75 ("Sutton has alleged sufficient facts, when accepted as true, to suggest an increased risk of future harm resulting from being implanted with St. Jude's device. Whether Sutton is likely to prevail on the merits is not a proper consideration at this time. We decline to preclude the possibility of a plaintiff or class of plaintiffs bringing suit under an increased risk of future harm theory due to the implantation of a medical device.").

41. *See Cent. Delta Water Agency*, 306 F.3d at 947–48 ("Because they use the water to irrigate their crops, plaintiffs contend that their ability to grow those crops will be severely hampered by the excessively saline water. The injury alleged has not yet occurred; it is threatened . . . . [W]e conclude that

ing where the defendant's violation of a National Pollutant Discharge Elimination System permit caused pollution of a waterway, which increased the risk of future harm to those downstream who used the waterway.[42] The *Pisciotta* court did not discuss why these cases provided support, but instead took it as self-evident that data breaches were analogous to these fact patterns and that therefore their reasoning could be utilized as support.[43]

The next circuit court to address the issue was the Ninth Circuit in 2010 with its decision in *Krottner v. Starbucks Corp*.[44] The plaintiffs in this case were some 97,000 "current or former Starbucks employees whose names, addresses, and social security numbers were stored on a laptop that was stolen from Starbucks."[45] The court in this case, citing *Pisciotta*, among other cases, found that the plaintiffs' allegations of future harm stemming from the theft of the laptop were sufficient to satisfy Article III's injury-in-fact requirement and confer standing.[46] The court reasoned that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data," and stated that had the "allegations [been] more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far

---

the necessary showing for standing purposes is not that the Vernalis standard has already been exceeded, or that plaintiffs' crops have already been damaged by excessively saline water, but that plaintiffs face significant risk that the crops that they have planted will not survive as a result of the Bureau's decisions to discharge water from the New Melones Reservoir during April, May, and October, rather than when needed to meet the Vernalis standard. The threat of injury resulting from the Bureau's employing an operational plan that will likely lead to violations of the Vernalis standard is sufficient to confer standing on plaintiffs.").

42. *See Friends of the Earth, Inc.*, 204 F.3d at 160 ("In this case, Gaston Copper's alleged permit violations threaten the waters within the acknowledged range of its discharge, including the lake on Shealy's property. By producing evidence that Gaston Copper is polluting Shealy's nearby water source, CLEAN has shown an increased risk to its member's downstream uses. This threatened injury is sufficient to provide injury in fact.").

43. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

44. *See* Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

45. *Id*. at 1140.

46. *Id*. at 1142–43 ("On these facts, however, Plaintiffs–Appellants have sufficiently alleged an injury-in-fact for purposes of Article III standing.").

less credible."[47] In support of its reasoning, this court utilized the *Pisciotta* review of analogous precedent in toxic substances, medical monitoring, and environmental harm cases.[48]

The Third Circuit, when faced with an identical Article III standing issue and a similar set of facts to those in *Pisciotta* and *Krottner*, came to the opposite conclusion when it decided *Reilly v. Ceridian Corp.* in 2011.[49] The plaintiffs in *Reilly* were a group of employees of the Brach Eichler law firm, which was a customer of Ceridian Corporation, a payroll-processing firm.[50] In December of 2009, Ceridian Corporation's data security was breached, allowing access to "personal and financial information belonging to . . . approximately 27,000 employees at 1,900 companies."[51] Included in the information accessed were the individuals' "first name, last name, social security number and, in several cases, birth date and/or the bank account that is used for direct deposit."[52] The injuries that the plaintiffs alleged to have incurred included, "an increased risk of identity theft, . . . costs to monitor their credit activity, and . . . emotional distress."[53] Like the plaintiffs in *Pisciotta* and *Krottner*, the plaintiffs did not allege any existing harm, only future harm and costs stemming from prophylactic preventative measures.[54] The *Reilly* court refused to confer Article III standing, reasoning that the allegations of future injury were "hypothetical," and "attenuated, because [they are] dependent on entirely speculative, future actions of an unknown

47. *Id*. at 1143.

48. *Id*. at 1142 ("The [*Pisciotta*] court surveyed case law addressing toxic substance, medical monitoring, and environmental claims in the Second, Fourth, Sixth, and Ninth Circuits. It concluded: 'As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions. We concur in this view. Once the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry.'" (citations omitted)).

49. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 41–42 (3d Cir. 2011).

50. *Id*. at 40.

51. *Id*.

52. *Id*.

53. *Id*.

54. *Id*. at 43 ("[A]ppellants in this case have yet to suffer any harm, and their alleged increased risk of future injury is nothing more than speculation.").

third-party."[55] Among this speculation, reasoned the court, was that the hacker "read, copied, and understood their personal information; . . . intends to commit future criminal acts by misusing the information; and . . . is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names."[56] The *Reilly* court distinguished the case in front of them from *Pisciotta* and *Krottner*, arguing that, "the threatened harms [in *Pisciotta* and *Krottner*] were significantly more 'imminent' and 'certainly impending' than the alleged harm here."[57] Furthermore, the *Reilly* court criticized the reasoning of the *Pisciotta* and *Krottner* courts for refusing to get to the bottom of the constitutional standing issue, stating that, "both courts simply analogized data-security-breach situations to defective-medical-device, toxic-substance-exposure, or environmental injury cases."[58]

---

55. *Id*. at 42 ("We conclude that Appellants' allegations of hypothetical, future injury are insufficient to establish standing. Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").

56. *Id*.

57. *Id*. at 44 ("In *Pisciotta,* there was evidence that 'the [hacker's] intrusion was sophisticated, intentional and malicious.' In *Krottner,* someone attempted to open a bank account with a plaintiff's information following the physical theft of the laptop. Here, there is no evidence that the intrusion was intentional or malicious. Appellants have alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was penetrated. Appellants' string of hypothetical injuries do not meet the requirement of an 'actual or imminent' injury." (alteration in original) (citations omitted)).

58. *Id*. at 44–45 ("First, in those cases, an injury has undoubtedly occurred. In medical-device cases, a defective device has been implanted into the human body with a quantifiable risk of failure. Similarly, exposure to a toxic substance causes injury; cells are damaged and a disease mechanism has been introduced . . . . Second, standing in medical-device and toxic-tort cases hinges on human health concerns. Courts resist strictly applying the 'actual injury' test when the future harm involves human suffering or premature death." (citations omitted)).

2. *Clapper* Holds That Future Harm Must be Certainly Impending to Satisfy Article III's Standing Requirement; Potentially Forecloses Data Breach Plaintiffs from Gaining Standing by Alleging Future Harm

In 2013, the United States Supreme Court decided *Clapper*; a case in which the issue of Article III standing based upon future harm was discussed in great detail.[59] The plaintiffs in this case were a group of U.S. citizens whose work put them in "international communications with individuals who they believe[d] [were] likely targets of surveillance under § 1881a."[60] Section 1881a is a part of U.S. intelligence law[61] that "allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States."[62] The plaintiffs argued that they could demonstrate the injury-in-fact necessary to establish Article III standing, "because there is an objectively reasonable likelihood that their communications will be acquired under § 1881a at some point in the future."[63] The Court held that the plaintiffs lacked Article III standing, "because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[64] In articulating the standard for Article III standing, the Court stated that, "we have repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[65] This language seemed to forestall allegations of future injury from satisfying Article III standing; indeed, many posited that *Clapper* could be the end of data breach litigation based on the

59. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146–55 (2013).
60. *Id*. at 1142.
61. Foreign Intelligence Surveillance Act of 1978 § 702, 50 U.S.C. § 1881a (2012).
62. *Id*. at 1142 (footnote omitted).
63. *Id*. at 1143.
64. *Id*. at 1155.
65. *Id*. at 1147 (alteration in original) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

threat of future injury and the prophylactic measures taken to prevent it.[66]

3. *Remijas*: the Circuit Split Survives *Clapper*

In the wake of *Clapper*, it seemed unclear whether data breach cases in which plaintiffs lack actual misuse of data would be able to survive a *Clapper* challenge to standing.[67] When the Seventh Circuit decided *Remijas* in July of 2015,[68] and Neiman Marcus Group, LLC's petition for a rehearing en banc was subsequently denied, it became clear to the legal world that data breach plaintiffs lacking a showing of actual data misuse could indeed satisfy the *Clapper* standing requirements and that the circuit split remained.[69] The plaintiffs in *Remijas* were a group of Neiman Marcus customers whose credit card numbers had potentially been exposed during a 2013 data security breach.[70] Among the issues that the *Remijas* court faced was whether to confer standing to the class members who were alleging that "un-reimbursed fraudulent charges and identity theft may happen in the future, and that these injuries are likely enough that immediate preventative measures are necessary."[71] In conferring standing to these plaintiffs, the *Remijas* court argued that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to sup-

66. *See Does Clapper Silence Data Breach Litigation? A Two-Year Retrospective*, *supra* note 9 (discussing the possibility that *Clapper* could silence data breach litigation).

67. *See* Heidi J. Milicic, *Standing to Bring Data Breach Class Actions Post-*Clapper, A.B.A. (Aug. 7, 2014), http://apps.americanbar.org/litigation/committees/commercial/articles/summer2014-0814-data-breach-class-actions-post-clapper.html ("Several defendants have seized upon the Supreme Court's decision in *Clapper* to challenge standing in data breach cases where the plaintiffs have not alleged actual misuse of the data. To date, virtually every defendant asserting a *Clapper*-based challenge has been successful. Federal courts in Illinois, New Jersey, Ohio, and the District of Columbia have interpreted *Clapper* to require dismissal of data breach lawsuits where the plaintiffs have not alleged actual misuse of the data. One California district court, however, found that standing existed even though the plaintiffs did not allege actual misuse of their data." (citation omitted)).

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

69. *See* Shepard, *supra* note 10.

70. *Remijas*, 794 F.3d at 690 ("In mid-December 2013, Neiman Marcus learned that fraudulent charges had shown up on the credit cards of some of its customers . . . . 350,000 cards were potentially exposed; and 9,200 of those 350,000 cards were known to have been used fraudulently.").

71. *Id*. at 692.

port Article III standing."[72] In defense of this, the court cited a footnote from *Clapper* that stated that a "substantial risk" of harm can sometimes suffice to confer standing.[73] In reasoning that the plaintiffs' risk of harm from the data breach was substantial, the court made the following argument: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[74] The court found that in this case, as opposed to in *Clapper*, "[t]he hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information," and that there was no speculation about whether the information was stolen and what was taken.[75] The court also cited as support a United States Government Accountability Office report which found that "stolen data may be held for up to a year or more before being used to commit identity theft [and] once stolen . . . fraudulent use of that information may continue for years."[76] In deciding that the plaintiffs should also be conferred standing for time and money lost to mitigation of future harm, the court reasoned that since there is a "substantial risk" that the harm will occur, this makes the harm imminent and therefore the mitigation expenses qualify as actual injuries.[77] In so reasoning, the court found it highly probative

---

72. *Id*. at 693.

73. *Id*. ("To the contrary, it stated that '[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In 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.'" (alteration in original) (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013))).

74. *Id*.

75. *Id*. ("The plaintiffs allege that the hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information. Whereas in *Clapper,* 'there was no evidence that any of respondents' communications either had been or would be monitored,' in our case there is 'no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken.'" (alteration in original) (quoting *Clapper*, 133 S. Ct. at 1148)).

76. *Id*. at 694 (quoting U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007)).

77. *Id*. ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent. Plaintiffs 'cannot manufacture standing by incurring costs in anticipation of non-imminent harm.' 'If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.' Once

that Neiman Marcus had offered free credit monitoring and identity theft protection to all of its customers who had shopped at the store during the time that the data breach was occurring.[78]

C. THE SIGNIFICANCE OF *SPOKEO, INC.* TO ARTICLE III STANDING IN DATA BREACH CASES

Spokeo, Inc. v. Robins is a case currently in front of the United States Supreme Court, which could have huge implications on the issue of Article III standing in data breach cases.[79] *Spokeo, Inc.* was granted certiorari out of the Ninth Circuit to resolve the issue of whether the plaintiff can maintain Article III jurisdiction based solely on the violation of a federal statute by Spokeo, Inc.—that is, without suffering any concrete harm.[80] Robins, the plaintiff and respondent in this case, is alleging that Spokeo, Inc., a website that "sells reports of aggregated, publicly available information about individuals,"[81] had compiled a report associated with his name which was available for purchase and contained inaccurate information about him, in contravention of the Fair Credit Reporting Act (FCRA), 15

---

again, however, it is important not to overread *Clapper*. *Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring." (citations omitted) (quoting *Clapper* 133 S. Ct. at 1151–52)).

78. *Id*. ("It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis* . . . . That easily qualifies as a concrete injury.").

79. Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014), *cert. granted*, 135 S. Ct. 1892 (U.S. Apr. 27, 2015) (No. 13-1339).

80. *See* Michelle W. Cohen & J. Taylor Kirklin, *What's at Stake in the Supreme Court's Decision in* Spokeo, Inc. v. Robins*?*, DATA SEC. L. BLOG (Sept. 21, 2015), http://datasecuritylaw.com/blog/whats-at-stake-in-the-supreme-courts-decision-in-spokeo-inc-v-robins/ ("*Spokeo, Inc. v. Robins*—which involves the question of whether Congress, by authorizing a private right of action based on a violation of a federal statute, can confer Article III standing upon a plaintiff who has suffered no concrete harm—is one of the most eagerly anticipated decisions from the Supreme Court's October 2015 term.").

81. *Id*.

U.S.C. § 1681.[82] Robins' suit was originally dismissed without prejudice for failure to establish standing;[83] this ruling was later reversed and remanded by the Ninth Circuit before the United States Supreme Court granted certiorari.[84] The Ninth Circuit reasoned that Congress intends to create a statutory right when it creates statutes with a private right of action, and that because Robins suffered an individualized harm from FCRA's violation, due to his "personal interests in the handling of his credit information,"[85] the violation of this statutory right was "sufficient to satisfy the injury-in-fact requirement of Article III."[86] If the United States Supreme Court were to uphold the Ninth Circuit's ruling on the issue and allow Article III standing based on the violation of a federal statute, plaintiffs in data breach litigation would simply need to show a violation of a federal statute which has a private right of action in order to gain standing.[87]

---

82. *Id*. ("Specifically, he claimed that Spokeo's report stated that Robins had a graduate degree (when he does not), that he was employed and wealthy (when he actually was unemployed), and that Robins was married with children (both inaccurate)."); *see generally* 15 U.S.C. §§ 1681–1681x (2012) (establishing requirements on credit reporting agencies).

83. *See* Robins v. Spokeo, Inc., No. CV10–05306, 2011 WL 11562151, at *1 (C.D. Cal. Sept. 19, 2011) ("[T]he Court reinstates the January 27, 2011 Order, which found that Plaintiff fails to establish standing. Among other things, the alleged harm to Plaintiff's employment prospects is speculative, attenuated and implausible. Mere violation of the Fair Credit Reporting Act does not confer Article III standing, moreover, where no injury in fact is properly pled. Otherwise, federal courts will be inundated by web surfers' endless complaints. Plaintiff also fails to allege facts sufficient to trace his alleged harm to Spokeo's alleged violations. In short, Plaintiff fails to establish his standing before this Court." (citations omitted)).

84. *See Spokeo, Inc.*, 742 F.3d at 413–14.

85. *Id*. at 413.

86. *Id*. at 412–14 ("First, Congress's creation of a private cause of action to enforce a statutory provision implies that Congress intended the enforceable provision to create a statutory right. Second, the violation of a statutory right is usually a sufficient injury in fact to confer standing . . . . The scope of the cause of action determines the scope of the implied statutory right. When, as here, the statutory cause of action does not require proof of actual damages, a plaintiff can suffer a violation of the statutory right without suffering actual damages . . . . Robins's personal interests in the handling of his credit information are individualized rather than collective. Therefore, alleged violations of Robins's statutory rights are sufficient to satisfy the injury-in-fact requirement of Article III." (citations omitted)).

87. "Forty-seven states . . . have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information," and with the proposal of the Data Security and Breach Notification Act of 2015 before Con-

D. STATE AND FEDERAL STATUTORY DATA BREACH LAW AND FTC REGULATION

With the burgeoning number of data breaches that have occurred in the United States, state and federal legislators have taken steps to solve the issue.[88] Although these statutes establish security measures, their main thrust is notification.[89] Most of these statutes do not establish a private right of action

---

gress, a federal notification statute could potentially follow. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; *but see* Grant Gross, *Proposed Data Breach Notification Bill Criticized as Too Weak*, CSO (Mar. 18, 2015, 12:57 PM), http://www.csoonline.com/article/2898809/data-breach/proposed-data-breach-notification-bill-criticized-as-too-weak.html.

88. *See Security Breach Notification Laws*, *supra* note 87 ("Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information."); Jeff Kosseff, *Analysis of White House Data Breach Notification Bill*, COVINGTON: INSIDE PRIVACY (Jan. 15, 2015), http://www.insideprivacy.com/uncategorized/analysis-of-white-house-data-breach-notification-bill/ ("On Monday, President Obama announced his proposal of the Personal Data Notification & Protection Act, which would set nationwide rules for data breach notifications and preempt the patchwork of state breach notification laws.").

89. *See* MINN. STAT. § 325E.61, subd. 1 (2014) ("Any person or business that . . . owns or licenses data that includes personal information, shall disclose any breach of the security of the system . . . to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This disclosure must be made in the most expedient time possible and without unreasonable delay . . . ."); MINN. STAT. § 325E.64, subd. 2 (2014) ("No person or entity . . . that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data . . . . A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction."); *see also* Hogan Lovells, *Data Security and Breach Notification Legislation Gaining Traction in Congress*, INT'L ASS'N PRIVACY PROFESSIONALS (Mar. 30, 2015), https://iapp.org/news/a/data-security-and-breach-notification-legislation-gaining-traction-in-congress/ ("The [Data Security and Breach Notification Act of 2015] requires covered entities to 'implement and maintain reasonable' security measures to protect personal information and establishes breach notification obligations for covered entities that suffer a data security breach."). *But see* Grant Gross, *Proposed Data Breach Notification Bill Criticized as Too Weak*, CSO (Mar. 18, 2015, 12:57 PM), http://www.csoonline.com/article/2898809/data-breach/proposed-data-breach-notification-bill-criticized-as-too-weak.html (criticizing the current federal bill for being weaker than many existing state laws and also for preempting those existing state laws).

for victims whose statutory rights have been violated, though some do.[90] It is possible that the Court will decide in *Spokeo, Inc.* to confer standing whenever a statute containing a private right of action is violated; therefore, those federal data breach statutes containing private rights of action may soon be utilized to confer Article III standing in data breach litigation cases.

The FTC has the authority to regulate cyber security issues via the FTC Act, which prohibits unfair and deceptive business practices.[91] The FTC has brought actions against many companies in response to actual or potential breaches of data security.[92] The FTC has a wide latitude of injunctive and equitable relief it can seek, including consumer redress and the issuance of fines for violations of settlement orders stemming from an action. The FTC cannot issue civil penalties pursuant to violations of this Act.[93] Significantly for plaintiffs, there is no citizen suit provision, which means that an affected consumer

---

90. *See* FLA. STAT. ANN. § 501.171(10) (West Supp. 2016) ("This section does not establish a private right of action."). *But see* CAL. CIV. CODE § 1798.84(b) (West 2009) ("Any customer injured by a violation of this title may institute a civil action to recover damages."). *See generally* STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS (2016), http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf (providing a table with excerpts of state and federal data security statutes, including whether they offer a private right of action).

91. *See* 15 U.S.C. § 45(a) (2012) (making unlawful and authorizing the FTC to prevent "unfair or deceptive acts or practices in or affecting commerce"); *id.* § 45 (n) (requiring the FTC to only declare practices unlawful if the practices cause "or are likely to cause substantial injury to consumers" and the consumers cannot "reasonably avoid[]" the injury themselves); *see also* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 246–49 (3d Cir. 2015) (affirming the FTC's authority to regulate a company's data security practices to ensure that they are reasonable and appropriate to protect consumers' data, and that the FTC can take action "before actual injury occurs").

92. *See generally Cases Tagged with Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 (last visited Feb. 20, 2016) (listing FTC data security enforcement cases).

93. *See* GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 5–7 (2014), https://www.fas.org/sgp/crs/misc/R43723.pdf ("The FTC Act authorizes the FTC to seek injunctive and other equitable relief, *including consumer redress*, for violations. *The FTC does not possess explicit authority to issue civil penalties for data security violations of the FTC Act and is limited to fining companies for violating a settlement order*. Fines issued by the FTC must reflect the amount of consumer loss. If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review." (emphasis added)).

would be out of luck unless the FTC decides to take an action. Since there have only been around sixty data breach actions taken by the FTC since 2000,[94] FTC action is not a common avenue of compensation for most data breach victims.

E. PROBLEMS RELATING TO DAMAGES AND CAUSATION STILL REMAIN FOR DATA BREACH PLAINTIFFS

Plaintiffs successfully alleging injuries sufficient for standing in data breach cases will still need to tackle problems relating to damages and causation. It is common for companies who have suffered a data breach to offer some sort of free credit monitoring to those individuals affected by the breach.[95] Furthermore, it is typical for banks and credit card companies to absorb the financial harm stemming from fraudulent charges.[96] With no out-of-pocket costs, plaintiffs will need to show how exactly they have suffered legitimate damages. There are many different theories of damages that have been put forward in data breach cases with little success to date.[97] Furthermore, when many breaches happen simultaneously, plaintiffs with multiple accounts breached at different companies may face a problem of proving that any one particular breach is the cause of their harm. Even though these problems are important in determining a plaintiff's ability to receive compensation from a data breach, they lie outside the scope of this Note.

---

94. *See Cases Tagged with Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 (last visited Feb. 20, 2016).

95. *See* Jeff John Roberts, *5 Ways a Firm Can Stop a Data Breach Lawsuit*, FORTUNE (Feb. 2, 2016, 9:08 AM), http://fortune.com/2016/02/02/data-breach-lawsuits/ ("Today, in the wake of a data breach, most retailers are quick to offer free access to services that monitor for credit and identity theft.").

96. *See Consumer Fraud*, DEBT.ORG, https://www.debt.org/credit/your-consumer-rights/fraud/ (last visited Feb. 20, 2016) ("Banks and card companies absorb most of the financial responsibilities for the fraud.").

97. *See* Paul G. Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRACTICAL L.J., Oct.–Nov. 2014, at 49, 53–54, https://www.bakerlaw.com/files/uploads/News/Articles/LITIGATION/2014/Karlsgodt-Lit_OctNov14_DataBreachFeature.pdf (discussing alternative theories of harm that have been tried for establishing standing and damages, including "[l]ost time and inconvenience," "[e]motional distress," the "[d]ecreased economic value of [personally identifiable information]," and being "[d]enied the benefit of the bargain").

II. ANALYSIS

A. ANALYZING THE FEDERAL CASE LAW: *PISCIOTTA*, *KROTTNER*, *REILLY*, AND *REMIJAS*

1. *Pisciotta* and *Krottner* Get the Answer Right but Utilize Faulty Reasoning

The courts in *Pisciotta* and *Krottner* each held that the future risk of harm was sufficient to confer Article III standing.[98] The *Pisciotta* court cites the reasoning of four circuit court cases involving future harm fact patterns in support of its contention that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendants actions."[99] Although not explicitly expounded by the court, one can infer that these cases are provided as persuasive precedent because the court finds the future harm fact patterns which form their subject matter to be analogous to the threat of future harm from the data breach at issue in *Pisciotta*. The issues discussed in these four cases include exposure to toxic substances (*Denney*), defective medical equipment (*Sutton*), potential crop loss (*Central Delta*), and environmental contamination (*Friends of the Earth*).[100] The *Krottner* court goes perhaps a step further than the *Pisciotta* court in its explanation of the analogy by explaining the reasoning utilized in these cases, before noting that the *Pisciotta* court had found the analogy to the data

98. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased future risk of identity theft resulting from a stolen laptop containing names, addresses and social security numbers of 97,000 employees was sufficient to establish Article III standing); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that an increased future risk of harm is sufficient to confer Article III standing).

99. *Pisciotta*, 499 F.3d at 634 & n.3 (citing the reasoning in Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006)); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 570–75 (6th Cir. 2005); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000)).

100. *Denney*, 443 F.3d at 264–65; *Sutton*, 419 F.3d at 574–75; *Cent. Delta Water Agency*, 306 F.3d at 947–48; *Friends of the Earth, Inc.*, 204 F.3d at 160. For additional discussion on the use of these cases in *Pisciotta*, see *supra* notes 36–43, 58 and accompanying text.

breach context compelling, and then ultimately agreeing with the *Pisciotta* court.[101]

Legal scholars differ on the value and usefulness of reasoning by analogy.[102] It seems clear, however, that regardless of how important or useful of a tool reasoning by analogy may be to legal reasoning in general, it is possible to misuse it. In fact, it is the very aspect which draws us towards the use of analogy in legal reasoning that should give us pause. Analogies are valued for their ability to draw out similarities between two related concepts; however, by highlighting the similarities, analogies tend to mask the differences. Furthermore, analogies are sometimes used to bolster what is in effect a weak argument.

The flaws of reasoning by analogy are exacerbated if the analogy is not thoroughly expounded, and as the *Reilly* court points out, the *Pisciotta* and *Krottner* courts applied minimal scrutiny to their analogy of data breaches to other future harm fact patterns.[103] The *Reilly* court goes on to critique two important differences between the data breach type case and cases involving exposure to toxic substances and defective medical

---

101. *See Krottner*, 628 F.3d at 1142 ("Thus, in the context of environmental claims, a plaintiff may challenge governmental action that creates 'a credible threat of harm' before the potential harm, or even a statutory violation, has occurred. Similarly, a plaintiff seeking to compel funding of a medical monitoring program after exposure to toxic substances satisfies the injury-in-fact requirement if he is unable to receive medical screening. In *Pisciotta v. Old National Bancorp*, the Seventh Circuit extended that reasoning to the identity-theft context, holding that plaintiffs whose data had been stolen but not yet misused had suffered an injury-in-fact sufficient to confer Article III standing." (citations omitted)).

102. *Compare* EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 1–2 (1947) ("The basic pattern of legal reasoning is reasoning by example. It is reasoning from case to case. It is a three-step process described by the doctrine of precedent in which a proposition descriptive of the first case is made into a rule of law and then applied to a next similar situation. The steps are these: similarity is seen between cases; next the rule of law inherent in the first case is announced; then the rule of law is made applicable to the second case." (footnotes omitted)), *with* RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 86, 90 (1990) ("[Reasoning by analogy] has . . . no definite content or integrity; it denotes an unstable class of disparate reasoning methods . . . . I merely question whether reasoning by analogy, when distinguished from logical deduction and scientific induction on the one hand and stare decisis on the other, deserves the hoopla and reverence that members of the legal profession have bestowed on it.").

103. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) (pointing out that "both courts simply analogized data-security-breach situations to defective-medical-device, toxic-substance-exposure, or environmental-injury cases" and describing both courts' rationales as "skimpy").

devices.[104] The court argues that toxic substance and defective medical device cases involve human health concerns and include an injury that has undoubtedly occurred; both of which are absent in the data breach cases.[105] The court next distinguishes data breaches from environmental contamination cases by arguing that in the latter branch of cases, "monetary compensation may not adequately return plaintiffs to their original position," whereas in data breach cases, they would.[106] Furthermore, the *Reilly* court points out that the instrumentality by which the future harm will occur differs between data breach cases and these others.[107] In data breach cases, the instrumentality is a human, whereas in the other cases the instrumentalities include toxins, medical equipment, and contaminants.[108] It is an error to assume that these disparate instrumentalities will work in a consistent manner. Although this Note argues for a conclusion in line with that arrived at by the courts in *Krottner* and *Pisciotta*, the flaws in the reasoning

---

104. *Id.* at 45.

105. *Id.* ("These analogies do not persuade us, because defective-medical-device and toxic-substance-exposure cases confer standing based on two important factors not present in data breach cases. First, in those cases, an injury has undoubtedly occurred. In medical-device cases, a defective device has been implanted into the human body with a quantifiable risk of failure. Similarly, exposure to a toxic substance causes injury; cells are damaged and a disease mechanism has been introduced. Hence, the damage has been done; we just cannot yet quantify how it will manifest itself. In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo . . . . Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker. Second, standing in medical-device and toxic-tort cases hinges on human health concerns. Courts resist strictly applying the 'actual injury' test when the future harm involves human suffering or premature death . . . . This case implicates none of these concerns. The hacker did not change or injure Appellants' bodies; any harm that may occur—if all of Appellants' stated fears are actually realized—may be redressed in due time through money damages after the harm occurs with no fear that litigants will be dead or disabled from the onset of the injury." (citations omitted)).

106. *Id.* ("As the Court of Appeals for the Ninth Circuit explained in *Central Delta Water Agency*, standing is unique in the environmental context because monetary compensation may not adequately return plaintiffs to their original position. In a data breach case, however, there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely—*if* the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment." (citation omitted)).

107. *Id.* (noting that "any damages that may occur [in the case at hand] are entirely speculative and dependent on the skill and intent of the hacker").

108. *Id.*

utilized by both courts results in an inadequately supported conclusion, and therefore support must be sought elsewhere.

2. *Reilly* Avoids the Analogy Pitfall but Reaches the Wrong Conclusion

The *Reilly* court steers clear of analogy for the most part in holding that the "Appellants' allegations of hypothetical, future injury do not establish standing under Article III"[109]—though the court's reasoning is not without its flaws. The *Reilly* court's main concern with the allegations is that they are hypothetical and rely on significant speculation.[110] According to the *Reilly* court, in order for the future injury being alleged to occur, the hacker must have "(1) read, copied, and understood their personal information; (2) intend[] to commit future criminal acts by misusing the information; and (3) [be] able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names."[111] Certainly these three conditions must be met for future harm to occur; however, these scenarios are not as speculative as the court would have the reader believe.

The least speculative of the bunch is the assumption that the hacker "intends to commit future criminal acts by misusing the information."[112] As the *Remijas* court so aptly puts it, "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[113] The data stolen in a data breach is often misused for personal gain by the hackers; however, there are instances where obtaining and abusing data is not the ultimate goal of the hack. For example, "zero day exploits," occur when a group hacks a company's security network in order to sell them information about where they are vulnerable and how to shore up these vulnerable areas.[114] However, if the true purpose of the

---

109. *Id*. at 41.

110. *See id.* at 42 ("Appellants' contentions rely on speculation that the hacker [will take a number of actions] . . . . Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").

111. *Id*.

112. *Id*.

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

114. *Compare* Numaan Huq, *Follow the Data: Dissecting Data Breaches and Debunking Myths*, TREND MICRO 23–35 (2015),

hack was one of these "zero day exploits," it would seem likely that company would want to bring this information to light, as it would cut against the assertion that the breached data is at risk of misuse.

Next is the question of whether the hacker "read, copied, and understood their personal information;"[115] the only information that we have from the *Reilly* case is that "all that is known is that a firewall was penetrated,"[116] and that "[i]t is not known whether the hacker read, copied, or understood the data."[117] It seems premature to dismiss the plaintiffs' suit based on this lack of particular knowledge when there has not been discovery and Ceridian Corporation is in control of all of the details about the breach; what is to stop Ceridian Corporation and other subsequent companies from not releasing the details of a data breach in the hopes of getting any subsequent claims thrown out at the pleading stage?

The third assumption that the appellants are making is that the hacker is "able to use [the] information to the detriment of Appellants by making unauthorized transactions in Appellants' names."[118] If the hacker is sophisticated enough to gain access to a company's secure data, it is not much of a stretch to assume that he or she is sophisticated enough to be able to utilize that data for personal gain. Barring any facts tending to show a hacker's lack of sophistication, it seems improper not to infer from the fact that the hacker has successfully executed a data breach that he or she has some level of requisite sophistication. Overall, this list of contentions that the

---

http://www.npr.org/sections/alltechconsidered/2016/03/22/471416946/from-reagans-cyber-plan-to-apple-vs-fbi-everything-is-up-for-grabs?sc=17&f=1001&utm_source=iosnewsapp&utm_medium=Email&utm_campaign=app (depicting ads on Deep Web marketplaces selling various personal information, including bank accounts, phone accounts, credit cards, and social security numbers), *with From Reagan's Cyber Plan to Apple Vs. FBI: 'Everything is up for Grabs'*, NATIONAL PUBLIC RADIO: FRESH AIR (Mar. 22, 2016), http://www.npr.org/sections/alltechconsidered/2016/03/22/471416946/from-reagans-cyber-plan-to-apple-vs-fbi-everything-is-up-for-grabs?sc=17&f=1001&utm_source=iosnewsapp&utm_medium=Email&utm_campaign=app (discussing how data breaches/hacks are sometimes done for reasons other than to use the data accessed for personal gain, including to conduct a 'zero day exploit,' to send a political message, and to embarrass the hacked party).

115. *Reilly*, 664 F.3d at 42.
116. *Id.* at 44.
117. *Id.* at 40.
118. *Id.* at 42.

Reilly court believes to be speculative and attenuated seems to be reasonably likely.

Contrary to the *Reilly* ruling, the benefit of the doubt at the pleading stage as to the level of sophistication of the hacker or the extent of access by the hacker in the course of a data breach should be given to the party with the least information, as they are least likely to be able to establish specific facts about the breach.[119] Forcing a plaintiff to allege with particularity facts about the data breach when the company holds all of the information about the breach threatens to turn away many deserving plaintiffs at the pleading stage.[120] It would be better, as a matter of policy, to give the benefit of any doubt to the data breach victims, as the company would be best able to bring to light particular facts to rebut these presumptions of requisite sophistication and extent of access. The contrary position would allow a situation at the pleading stage where "[t]he required evidence will remain safely in wrongdoers' files, hidden from public view."[121]

2. *Remijas* Gets the Reasoning and the Conclusion Right

The *Remijas* court also steers clear of analogy, but seems more willing to make some of the plausible inferences that the *Reilly* court refused to make. The *Remijas* court infers from the fact that there has been a data breach that the perpetrator intends to and is able to utilize this information for personal gain.[122] This inference is a critical one, and the reluctance of

---

119. *See generally* WILLIAM FUNK ET AL., CTR. FOR PROGRESSIVE REFORM, PLAUSIBILITY PLEADING: BARRING THE COURTHOUSE DOOR TO DESERVING CLAIMANTS 1 (2010), http://www.progressivereform.org/articles/Twombly_1005.pdf ("The practical effect of the heightened pleading standard is that many deserving plaintiffs will be unable to have their claims heard in court, since they will not have access to any crucial facts that the defendant is able to keep out of public view. As such, the plausibility pleading standard places a nearly impossible burden on many deserving plaintiffs, making it significantly harder for them to get past the pleadings stage of civil litigation. As one might expect, valid complaints will often be wrongly dismissed if plaintiffs are required to prove factual allegations before having an opportunity to gather evidence. The required evidence will remain safely in wrongdoers' files, hidden from public view.").

120. *See id*.

121. *Id*.

122. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers'

the *Reilly* court to infer the same is a main reason why the courts came to different conclusions on whether or not future harm is imminent.[123] The *Remijas* court also cites a United States Government Accountability Office report that tends to support the proposition that harm from data breaches can commonly occur up to a year or longer from the date of the breach.[124] Furthermore, the *Remijas* court is more willing to consider prophylactic measures taken to prevent future harm stemming from a data breach as an injury.[125]

There are several aspects of the *Remijas* case that likely made it easier for the court to find standing as opposed to the case the *Reilly* court was considering. For one, there was particularity and conviction in the knowledge of what information had been hacked in *Remijas*[126] that was apparently lacking in *Reilly*;[127] though, as I have argued above, this lack of particularity should have been given less weight than it was given in *Reilly*. Furthermore in *Remijas*, 9200 cards had already been fraudulently charged, whereas there were no reported abuses of the breached data in *Reilly*.[128] This is a fact which the *Remijas* court found highly probative of a risk of future harm, and which the *Reilly* court lacked.[129] Although there were differ-

---

private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

123. *Compare id*. (describing the risk of future harm as "plausible"), *with Reilly*, 664 F.3d at 43 (describing the risk of future harm as "nothing more than speculation").

124. *See Remijas*, 794 F.3d 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. It cites a Government Accountability Office Report that finds that 'stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.'" (citing U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 76, at 29)).

125. *See id*. at 694 ("In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring.").

126. *See id*. at 693 ("[I]n our case there is 'no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken.'" (alternation in original)).

127. *See Reilly*, 664 F.3d at 40, 44 ("[A]ll that is known is that a firewall was penetrated . . . . It is not known whether the hacker read, copied, or understood the data.").

128. *See Remijas*, 794 F.3d at 690; *Reilly*, 664 F.3d at 43.

129. *See Remijas*, 794 F.3d at 692–93.

ences in fact, a main takeaway from comparing these two cases is that the *Remijas* court was willing to infer that the hacker performed the data breach with malicious intent,[130] whereas the *Reilly* court refused to make the same inference.[131] This is a crucial difference in reasoning which is likely to continue to divide these courts if not decided outside of the federal circuit courts.

B. *SPOKEO, INC.* COULD SETTLE THE ISSUE

As discussed earlier, it is possible that this issue could become much less contentious depending on how the United States Supreme Court rules in the *Spokeo, Inc.* case currently in front of it.[132] A ruling in line with the Ninth Circuit in *Spokeo, Inc.* is likely to remove some of the Article III standing roadblocks that data breach litigation plaintiffs currently face. The question presented in *Spokeo, Inc.* is, "Whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute."[133] A broad ruling would all but eliminate the Article III standing requirement as long as a plaintiff could establish that a company had violated a federal statute which included a private right of action.[134] Because a large number of federal statutes provide statutory damages for their violations, many are leery that a broad ruling could have a devastating effect on the busi-

---

130. *See id*. ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

131. *See Reilly*, 664 F.3d at 44 ("Here, there is no evidence that the intrusion was intentional or malicious.").

132. *See* Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014), *cert. granted*, 135 S. Ct. 1892 (U.S. Apr. 27, 2015) (No. 13-1339); *see also* discussion *supra* notes 79–86 and accompanying text.

133. Petition for Writ of Certiorari, *Spokeo, Inc.,* 135 S. Ct. 1892 (No. 13-1339).

134. *See generally* Cohen & Kirklin, *supra* note 80 ("Spokeo asserts that, if the Ninth Circuit's decision is not overturned, the Article III standing requirements would devolve into an 'empty formality' . . . .").

ness world.[135] It is also possible for the Court to effectively overrule *Remijas*, depending on how they word their opinion.

C. IF THE ISSUE REMAINS UNSETTLED POST-*SPOKEO, INC.*, THE UNITED STATES SUPREME COURT SHOULD GRANT CERTIORARI, IF AN OPPORTUNITY ARISES, AND ADOPT A HOLDING IN LINE WITH THAT OF THE *REMIJAS* COURT

Before the recent passing of United States Supreme Court Justice Antonin Scalia,[136] the trend of the United States Supreme Court had been to side with corporations.[137] With Justice Scalia's passing, that trend could potentially change; though of course the outcome for *Spokeo, Inc.* is far from certain.[138] If *Spokeo, Inc.* nevertheless comes out against the Ninth Circuit, then the issue of this Note, whether Article III standing should be conferred in data breach litigation cases when the plaintiff(s) allege only potential future harm or the prophylactic measures taken to prevent this potential future

---

135. *See, e.g.*, James E. Tysse et al., *In Potentially Significant Case, Supreme Court to Test Limits Of Privacy and Data Breach Class Actions Seeking Statutory Damages*, BLOOMBERG BNA (June 12, 2015), http://www.bna.com/potentially-significant-case-n17179927616/ ("Beyond FCRA and RESPA, statutory damages provisions are integral parts of the Fair Debt Collection Practices Act, the Lanham Act, the Truth in Lending Act, the Fair and Accurate Credit Transactions Act, the Telephone Consumer Protection Act, the Video Privacy Protection Act, the Electronic Communications Privacy Act, the Stored Communications Act and the Cable Communications Privacy Act, among others. Such provisions are also embedded in laws of general applicability—including the Employee Retirement Income Security Act and the Americans with Disabilities Act—meaning virtually every major American company is vulnerable. And because these laws often provide statutory damages of $1,000 or more per violation, some defendants may face massive liability for technical violations of federal law that result in no real harm.").

136. *See* Gary Martin & Guillermo Contreras, *U.S. Supreme Court Justice Antonin Scalia Found Dead at West Texas Ranch*, MYSANANTONIO.COM (Feb. 16, 2016, 1:52 PM), http://www.mysanantonio.com/news/us-world/article/Senior-Associate-Justice-Antonin-Scalia-found-6828930.php.

137. *See* Lee Epstein, William M. Landes & Richard A. Posner, *How Business Fares in the Supreme Court*, 97 MINN. L. REV. 1431, 1472 (2013) ("We find that five of the ten Justices who, over the span of our study (the 1946 through 2011 Terms), have been the most favorable to business are currently serving, with two of them ranking at the very top among the thirty-six Justices in our study.").

138. *Cf. id.* at 1450 (ranking Justice Scalia as the ninth most business friendly United States Supreme Court Justice in the period from 1946 to 2011).

harm, will remain split in the circuit courts.[139] If this is the case, the best solution is for the United States Supreme Court to address this issue directly at a later date.

1. This Issue is Proper for Certiorari

There are many factors which the United States Supreme Court considers when it decides whether or not to grant certiorari; one of these factors is whether a circuit split exists on an important issue.[140] It is unlikely that the *Reilly* and *Remijas* courts' will vacate their opinions or otherwise rule in contravention to their holdings in these cases; as such, the circuit split is likely to remain. It is worth noting that the circuit split predated *Clapper*,[141] and that although *Clapper* affected district court rulings significantly, it seems to have affected only the style of reasoning in federal circuit cases rather than determining the outcome.[142] Furthermore, the vast amount of data breaches that have occurred in the last decade, and the ensuing torrent of litigation that typically follows, speaks towards the importance of this issue.[143]

Because each of the federal circuit court data breach cases discussed in this Note are past the time allotted for filing a writ

---

139. *See* cases cited *supra* note 7.

140. *See* SUP. CT. R. 10 ("Review on a writ of certiorari is not a matter of right, but of judicial discretion. A petition for a writ of certiorari will be granted only for compelling reasons. The following, although neither controlling nor fully measuring the Court's discretion, indicate the character of the reasons the Court considers: (a) a United States court of appeals has entered a decision in conflict with the decision of another United States court of appeals on the same important matter.").

141. The Third Circuit split from the Ninth and Seventh in 2011. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased future risk of identity theft was sufficient to establish Article III standing), *and* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (same), *with* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (holding that allegations of possible future injury stemming from a data breach were not sufficient to satisfy Article III standing because the threatened injury was not certainly impending).

142. The Seventh Circuit kept same viewpoint in *Remijas* as it had before *Clapper*. *Compare* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015), *with Pisciotta*, 499 F.3d at 634. But the *Remijas* court used a more refined reasoning. *See* discussion *supra* notes 122–131 and accompanying text.

143. *See supra* text accompanying note 14.

of certiorari, the Court will need to wait for a new case to be able to grant certiorari.[144]

2. If an Opportunity Arises, the Court Should Adopt a Ruling in Line with the *Remijas* Court

If certiorari is granted for a subsequent data breach case, the Court should adopt a ruling in line with the reasoning of the *Remijas* court. Unlike the *Pisciotta* and *Krottner* courts, the *Remijas* court does not make use of misguided analogies to other future harm cases.[145] Furthermore, the *Remijas* court correctly identifies that the fact that a data breach has occurred is evidence of the hacker's malicious intent to use the data for personal gain and to the detriment of the individuals whose data has been breached.[146]

In addition to the reasoning of the *Remijas* court, the court's holding seems superior to *Reilly*'s from a policy standpoint. In *Reilly*, the court found the plaintiffs' lack of particular knowledge about the extent of access by the hacker, and the hacker's level of sophistication, as probative of the lack of certainty that harm was imminent.[147] It seems prudent that, should any doubt exist as to particular facts about the breach at the pleading stage, the benefit of this doubt should be given to the party who is least able to establish specific facts about

144. *See* 28 U.S.C. § 2101(c) (2012) ("Any other appeal or any writ of certiorari intended to bring any judgment or decree in a civil action, suit or proceeding before the Supreme Court for review shall be taken or applied for within ninety days after the entry of such judgment or decree. A justice of the Supreme Court, for good cause shown, may extend the time for applying for a writ of certiorari for a period not exceeding sixty days.").

145. *See Krottner*, 628 F.3d at 1142 ("The [*Pisciotta*] court surveyed case law addressing toxic substance, medical monitoring, and environmental claims in the Second, Fourth, Sixth, and Ninth Circuits. It concluded: 'As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions. We concur in this view. Once the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry.'" (citations omitted)).

146. *See Remijas*, 794 F.3d at 693 ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

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

the breach.[148] The *Reilly* court's position to the contrary would likely incentivize companies to be secretive about the extent and sophistication of a breach in the hopes that they could turn the suit away at the pleading stage.[149] By making the reasonable assumption, as the *Remijas* court did, that hackers are able to decipher the data they encounter, intend to misuse that information for personal gain, and are likely sophisticated enough to do so,[150] the burden of rebutting these presumptions is properly placed with the party which holds all of the information which could potentially be provided for rebuttal.

3. Other Solutions are Unlikely to Address the Litigation Issue

State and federal statutes' focus on notification makes them a poor avenue for consumers seeking remedial action.[151] The intent of these statutes is to incentivize companies to take preventative measures against data breaches.[152] While these statutes serve to prevent future incidents of data breach, it is unlikely to result in any redress for individuals who have already suffered identity or financial data theft, as many of these statutes lack a private right of action.[153]

---

148. *Cf.* FUNK ET AL., *supra* note 119, at 6 ("[Heightened pleading standards] rob[] plaintiffs of the benefit of the longstanding rule requiring judges to draw all reasonable inferences in favor of the plaintiff. Judges have long given plaintiffs the benefit of the doubt in this manner . . . ." (footnote omitted)).

149. *Cf. id.* at 1 ("The practical effect of the heightened pleading standard is that many deserving plaintiffs will be unable to have their claims heard in court, since they will not have access to any crucial facts that the defendant is able to keep out of public view . . . . As one might expect, valid complaints will often be wrongly dismissed if plaintiffs are required to prove factual allegations before having an opportunity to gather evidence. The required evidence will remain safely in wrongdoers' files, hidden from public view.").

150. *See Remijas*, 794 F.3d at 693.

151. *See generally* STEPTOE & JOHNSON LLP, *supra* note 90 (noting few statutes providing a private right of action); *Security Breach Notification Laws*, *supra* note 87 (providing a list of notification-based statutes).

152. *See* Pam Greenberg, *Right to Know*, ST. LEGISLATURES MAG., Dec. 2008, at 26, 27 http://www.ncsl.org/Portals/1/Documents/magazine/articles/2008/08sldec08_right.pdf ("The law also creates a powerful incentive on the part of government and business to improve data security. . . . Companies have increased security practices in response to data breach laws, according to Chris Hoofnagle, director of Information Privacy Programs at the Berkeley Center for Law & Technology, who supervised a survey of chief security officers by the Samuelson Clinic.").

153. *See id.* at 28 ("[T]he effectiveness of data breach laws on these [identity] thefts is limited . . . . [But] security breach laws may have other benefits, such as reducing a victim's average losses and improving security practices.");

The FTC has the authority to regulate data security pursuant to a FTC Act prohibiting unfair practices.[154] Though the FTC has been active in bringing administrative enforcement actions over data breach issues, it lacks the authority to issue civil penalties.[155] In order for the FTC to fine a company pursuant to this Act, the company must be in violation of a settlement order.[156] The FTC has the ability to force a company to reimburse its consumers after a data breach; however, the FTC decides which actions it will pursue, meaning that many data breach victims' cases are not pursued by the FTC. This makes FTC action a poor source of recovery for most plaintiffs who have suffered damages from a data breach.

CONCLUSION

Data breaches have affected hundreds of millions of Americans,[157] with several hundred occurring just last year.[158] Litigation usually follows a data breach like a tail follows a dog; however, data breach plaintiffs have faced common roadblocks.[159] Article III requires a showing of an injury-in-fact that is "concrete, particularized, and actual or imminent."[160] This Note discussed the federal circuit court split on the issue of whether plaintiffs can satisfy Article III's standing requirement while alleging only future harm or harm based on prophylactic measures taken to protect against future harm, notably *Reilly* and *Remijas*. This Note further discussed the relevance of the United States Supreme Court cases *Clapper* and *Spokeo, Inc.*, the latter of which is currently pending.

This Note argued that the threat of future harm in data breach cases, and the prophylactic measures taken to protect against this future harm should satisfy the injury-in-fact requirement of Article III standing. Furthermore, it argued that if *Spokeo, Inc.* does not solve the issue, ultimately, the United States Supreme Court should, if an opportunity arises, resolve

---

see, e.g., FLA. STAT. ANN. § 501.171(10) (West Supp. 2016) ("This section does not establish a private right of action.").

154. *See* discussion *supra* notes 91–93 and accompanying text.

155. *See* STEVENS, *supra* note 93.

156. *Id.*

157. The number of records breached in the Healthcare sector alone numbered over 112 million in 2015. Munro, *supra* note 3.

158. *See Identity Theft*, *supra* note 2.

159. *See* Post, *supra* note 4.

160. *See* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).

this circuit split and adopt a ruling similar to that of the *Remijas* court. The *Remijas* ruling has superior reasoning, and makes for better policy, which make it more appealing than its counterparts: *Reilly*, *Krottner*, and *Pisciotta*. *Remijas*, unlike *Krottner* and *Pisciotta*, does not depend on a thinly constructed analogy to other future harm cases, an analogy that this Note has argued does not stand up to scrutiny. Although *Reilly* also steered clear of this unsubstantiated argument by analogy, this Note has argued that the reasoning in *Remijas* is superior. Most notably, the *Remijas* court made the crucial inference that a hacker who conducts a data breach likely intends to use the data they access for personal gain and to the disadvantage of those whose data was breached. The *Reilly* court refused to make the same inference, arguing that it was indeterminate as to what the hacker's motivation was in executing the breach, as to what the extent of the breach was, and as to what the hacker intended to do with the data they acquired. Furthermore, the *Remijas* court, in opposition to the *Reilly* court, appears to give the benefit of the doubt concerning the details of the data breach to the plaintiffs; this seems proper at the pleading stage, as there has been no discovery and one party is in control of all of the data. Finally, United States Supreme Court action on this issue is desirable because other legal solutions seem unlikely to address the issue for ongoing and future data breach litigation. The state and federal statutes focus primarily on notification and typically lack a private right of action, and the FTC, though it has the authority to regulate, and has regulated extensively in the data security realm, remains a poor avenue for most data breach victims seeking compensation.

***