The John Marshall Journal of Information Technology & Privacy Law

Volume 32 | Issue 4 Article 3

Spring 2016

The Presumption of Injury: Giving Data Breach Victims "A Leg To Stand On," 32 J. Marshall J. Info. Tech. & Privacy L. 301 (2016)

Corey Varma

COMMENTS

THE PRESUMPTION OF INJURY: GIVING DATA BREACH VICTIMS "A LEG TO STAND ON"[1]

COREY VARMA*

INTRODUCTION

It begins when you receive a letter from a company that has suffered a data breach. The letter explains, in a conciliatory tone, that the attacker responsible for the data breach has unlawfully gained access to information on the company's servers. Though the company has patched the vulnerability that allowed the attacker to access your personally identifiable information ("PII"), the attacker has already accessed it. The PII that the attacker accessed includes your name, email address, phone number, Social Security number, credit card numbers, and a myriad of other sensitive information.[2] While the company might offer you free credit monitoring, you still feel violated.

Data breaches have increasingly become an all too common occurrence. News outlets referred to 2014 as the "year of the data breach"[3] with over 783 major data breaches.[4] But these breaches are nothing new; according to the Privacy Rights Clearinghouse, since 2005 hackers compromised approximate-

---

* Corey Varma is originally from Orange County, California, where he received his undergraduate education at California State University, Fullerton, earning a BA in Psychology. Corey moved to Chicago in pursuit of a career in the law, and is a 2017 JD Candidate at The John Marshall Law School in Chicago, Illinois. He is enormously grateful to his family and friends for their constant support and encouragement during his journey through law school. Corey would also like to thank the 2015-2016 Editorial Board of the Journal of Information Technology & Privacy Law for their constant guidance throughout the writing of this work.

1. RICHARD A. SPEARS, MCGRAW-HILL'S AMERICAN IDIOMS DICTIONARY 357 (4th ed. 2007) ("[for an argument or a case] to have no support") (brackets in original).

2. Among the sensitive information compromised in data breaches is health information. The health care sector ranked second highest for data breaches in 2015, accounting for "35.5 percent of the total overall breaches." *Identity Theft Resource Center Breach Report Hits Near Record High in 2015*, IDENTITY THEFT RES. CTR. (Jan. 25, 2016), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

3. Bill Whitaker, *What happens when you swipe your card?*, CBS NEWS (Nov. 30, 2014),http://www.cbsnews.com/news/swiping-your-credit-card-and-hacking-and-cybercrime/ ("2014 is becoming known as the 'year of the data breach.'"); Tara Seals, *Breach Fatigue? Most Consumers Unaware of eBay, Home Depot Incidents*, INFOSECURITY MAG. (Oct. 3, 2014), http://www.infosecurity-magazine.com/news/consumers-unaware-of-ebay-home/ ("2014 has been dubbed the year of the data breach.").

4. *Identity Theft Resource*, *supra* note 2.

ly 895,508,931 individual records across 4,669 data breaches.[5] Those numbers are expected to grow, while 2015 was also referred to as "year of the data breach."[6]

Unfortunately, individuals who have their PII compromised by a data breach lack a proper recourse. While lawsuits tend to follow quickly after a data breach,[7] few suits successfully survive a motion to dismiss.[8] The typical data breach lawsuit is filed within days of a company's official announcement that it has been breached,[9] and frequently before there is any indication that the attacker has misused the stolen PII.[10]

In these lawsuits, the plaintiffs often allege that the defendant company's negligence in securing their computer systems caused the data breach and subsequent compromise of the plaintiffs' PII, exposing the plaintiffs to injury, principally through the risk of future identity theft.[11] However, in this common scenario, the defendant company will likely argue the plaintiffs lack standing under FED. R. CIV. P. 12(b)(1),[12] though the success of this argument depends on where the plaintiffs filed the suit.[13]

This outcome is wrong because our society has increasingly embraced technology. And although technology has undoubtedly made our lives more convenient, it also opens up our society to unprecedented costs and inconveniences by way of identity theft and credit card fraud without a straightforward or accessible means to remediate those costs or inconveniences within our legal framework.

In 2011, one researcher estimated the average Internet user was responsible for over 3,300 transactions per day.[14] Considering the proliferation of Internet connected mobile phones, that number is presumably much higher today. Many of these transactions on the Internet include sensitive PII that finds its way into databases that are vulnerable to data breaches.[15]

But the Internet is not unique when it comes to data breaches. Many

---

5. *Chronology of Data Breaches from 2005 to Present*, PRIVACY RIGHTS CLEARINGHOUSE http://www.privacyrights.org/data-breach (last visited Nov. 25, 2015).

6. *Raytheon Websense Predicts 2016 Cybersecurity Threat Landscape*, FORCEPOINT (DEC 2, 2015), https://blogs.forcepoint.com/press-releases/raytheonwebsense-predicts-2016-cybersecurity-threat-landscape; Tal Kopan, *Hack Friday*, POLITICO (Nov. 28, 2014), http://www.politico.com/story/2014/11/black-friday-cybercrime-113192.

7. News reports of the hack began coming in on December 18, 2016. Target sent a data breach notification to their customers via email on December 20, 2013. And the first lawsuit against Target was filed that same day on December 20, 2013. *See* Class Action Complaint, *Purcell v. Target Corp.*, 3:13-cv-02274-JE (D. Or. 2013).

8. *See e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011).

9. *See* Class Action Complaint, *Purcell v. Target Corp.*, 3:13-cv-02274-JE.

10. *Id.*

11. *See e.g.*, *Reilly v. Ceridian Corp*.

12. *Enslin v. Coca-Cola Co.*, 2015 U.S. Dist. LEXIS 133168, *8 (E.D. Pa. 2015) ("A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) if the plaintiff lacks standing under Article III of the constitution.")(citing *Steel Company v. Citizens for a Better Environment*, 523 U.S. 83, 101-02 (1998)).

13. *Katz v. Pershing*, 672 F.3d 64, 80 (1st Cir. 2012).

14. *Web Transactions Per User Per Day*, ZSCALER (Jan. 25, 2011), http://research.zscaler.com/2011/01/web-transactions-per-user-per-day.html ("The average for this data sample was: 3343.80227 web transactions per user per day").

15. For example, logging into your online banking or accessing your online medical record requires many individual transactions and logging of sensitive PII in databases. *See generally id*.

commonplace transactions, ranging from swiping your credit card at a store[16] to making a deposit at a bank,[17] can make an individual's PII vulnerable to a data breach. Take the 2014 Target data breach for example.[18] The credit card numbers and other PII taken from Target's databases were all from physical interactions as opposed to online sales.[19] The Target data breach compromised about 70 million records in total.[20]

As data breaches become more frequent, and their serious effects become more widespread, our legal framework should be reevaluated. The courts must act to establish a cogent and uniform standard for data breach standing that would allow individuals affected by data breaches to argue their cases on the merits. Rather than being turned away at the courthouse steps it would allow victims to seek redress from companies that failed to take reasonable steps to secure individuals' PII. Such a uniform standard for standing would also serve public policy by stressing corporate liability for data breaches, motivating businesses to secure their customers' PII.

In addressing the issues presented, Part I of this comment provides background to the general requirement for Article III standing. Part II will examine representative data breaches previously litigated, paying close attention to their respective outcomes to assess why some courts are reluctant to grant standing to data breach plaintiffs. Part III of this comment will draw important distinctions between data breach cases and data collection cases. Part IV of this comment will propose a new approach to standing for litigation following a data breach, while examining the justiciability, fairness, and public policy implications of the proposal. And finally, Part V of this comment will describe how this new approach to standing for data breach litigation will apply in the typical lawsuit following a data breach.

I

BACKGROUND

Article III, Section 2, Clause 1 of the United States Constitution defines the baseline for standing in Federal courts.[21] This clause of the Constitution is commonly referred to as the case-or-controversy requirement.[22] It works to limit the Court's jurisdiction to actual cases or controversies.[23] The Supreme

16. Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES (Jan. 10, 2014), http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

17. Tanya Agrawal, David Henry & Jim Finkle, *JPMorgan hack exposed data of 83 million, among biggest breaches in history*, REUTERS (Oct. 2, 2014), http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003.

18. Harris & Perlroth, *supra* note 16.

19. *Id.*

20. *Id.*

21. U.S. Const. art. III, § 2, cl. 1.

22. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) ("[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III"); *see also* U.S. Const. art. III, § 2, cl. 1.

23. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013) ("Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'"); *see also North*

Court has since raised the threshold of this baseline for standing, making it more difficult for plaintiffs to meet Federal court standing requirements.[24] In order to gain standing under contemporary standing jurisprudence, a plaintiff's "injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action [(causation)]; and redressable by a favorable ruling.'"[25]

The injury element can pose considerable difficulty for data breach plaintiffs. Though, the latter two requirements of causation[26] and redressability[27] are generally easy to demonstrate in data breach litigation. As such, this comment will principally focus on the injury requirement for standing. Specifically, this comment will focus on the injury caused by the imminent, and arguably overwhelming, increased risk of identity theft that follows a data breach perpetrated by an unknown hacker.

There is considerable disagreement amongst the courts as to the applicability of this increased risk of identity theft theory of injury in data breach cases.[28] The First Circuit Court of Appeals, citing to decisions from various other circuits, acknowledged the "disarray about the applicability of this sort of 'increased risk [of identity theft]' theory in data privacy cases."[29] This "disarray" leads to data breach cases being dismissed because, according to some courts, an increased risk of identity theft is not a sufficient injury to confer Article III standing.[30] Yet other courts have found this "increased risk" theory sufficient to confer Article III standing, which permits the case to be heard on

---

American Natural Resources, Inc. v. Strand, 252 F.3d 808, 812 (6th Cir. 2001) ("One of the fundamental axioms of American jurisprudence is that a federal court may consider only actual cases or controversies.").

24. *Lujan v. Defenders of Wildlife*, 504 U.S. at 562 (citations omitted).

25. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. at 1147 (2013) (citing *Monsanto Company v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)) (internal quotation marks omitted).

26. A plaintiff can readily show the defendant company was the cause of the data breach by demonstrating the data breach would not have occurred but for the company's failure to ensure the security of the plaintiffs' PII. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327-28 (11th Cir. 2012) ("Because their contention that the data breach caused the identity theft is plausible under the facts pled, Plaintiffs meet the pleading standards for their allegations."); *see also In re Zappos.com, Inc.*, 2015 U.S. Dist. LEXIS 71195, *30 (D. Nev. 2015) ("Since today so much of our personal information is stored on servers just like the ones that were hacked in this case, it is not unrealistic to wonder whether Plaintiffs' hypothetical future harm could be traced to Zappos's breach.").

27. Plaintiffs can usually allege statutory damages, common law tort doctrines, or request compensation for the cost of the data breach to establish redressability. *See* Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1371 (2013), *available at* http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1889&context=aulr ("The credit-monitoring injunctive relief approved by multiple courts in settlement proceedings between data breach claimants and data storage entities suggests that the threat of identity theft is a remediable injury with concrete available relief.").

28. *Katz v. Pershing*, 672 F.3d at 80.

29. *Id.*

30. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,* 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("increased risk of harm alone does not constitute an injury in fact."); *Reilly v. Ceridian Corp.*, 664 F.3d at 42 ("We conclude that Appellants' allegations of hypothetical, future injury are insufficient to establish standing."); *In re Zappos.com, Inc.*, 2015 U.S. Dist. at *25 ("The Court therefore finds that the increased threat of identity theft and fraud stemming from the Zappos's security breach does not constitute an injury-in-fact sufficient to confer standing.").

its merits.[31]

The most widely cited decision in regard to the injury requirement of standing is *Clapper v. Amnesty Int'l*, where the United States Supreme Court examined the issue of standing in the context of data collection.[32] At issue in *Clapper* was the National Security Agency's ("NSA") warrantless wiretapping of telephone and e-mail communications (or "data collection").[33] The plaintiffs in *Clapper* were attorneys who believed their clients were the targets of this data collection. They alleged their communications were the target of Government surveillance and as a result, "at some point in the future," they would suffer an injury.[34] Additionally, they alleged a present harm that "the risk of surveillance [by the NSA] is so substantial that they have been forced to take costly and burdensome measures to protect the confidentiality of their [...] communications."[35]

The majority of the Court in *Clapper* found that the plaintiffs lacked standing because there was no indication that the NSA was actually targeting them, stating that the plaintiffs' injuries were "mere speculation."[36] Further, as to the "costly and burdensome measures" the plaintiffs took to protect their communications, the Court found that the plaintiffs lacked standing because they were "inflicting harm on themselves based on their fears of hypothetical future harm."[37]

Data breach decisions that cite to *Clapper* dismiss data breach claims for similar reasons, finding that plaintiffs are merely speculating as to whether an attacker has actually accessed or misused their personal information, until the plaintiffs experience actual identity theft.[38] These courts additionally define any prophylactic measures taken by the plaintiffs (such as credit monitoring) as self-inflicted injuries that do not merit the conferral of standing.[39] However, the data breach decisions citing to the standard set forth in *Clapper* are wrong because data breach is not data collection.

Data collection is defined as "systematically collecting [...] records in bulk."[40] Data collection is commonly referred to as wiretapping[41] and is most

---

31. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692 (7th Cir. 2015) ("*Remijas II*")("The plaintiffs also allege that they have standing based on two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) ("Here, Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.").

32. *See generally Clapper v. Amnesty.*

33. *Id.* at 1143-44.

34. *Id.* at 1144.

35. *Id.*

36. *Id.* at 1148.

37. *Id.* at 1144.

38. *See, e.g.*, *In re Zappos.com* at *25-26 ("The degree of Plaintiffs' speculation is heightened further by the fact that the future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor. Should the person or persons in possession of Plaintiffs' information choose not to misuse the data, then the harm Plaintiffs fear will never occur. Likewise, if the person or persons in possession of Plaintiffs' information are unable to use the data to wreak the havoc assumedly intended, then Plaintiffs' alleged damages would also not coalesce.").

39. *Clapper v. Amnesty* at 1152.

40. Charlie Savage & Jonathan Weisman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. TIMES (May 7, 2015), http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html.

often conducted in connection with national security efforts[42] or online marketing.[43] On the contrary, data breach is defined as "[t]he unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information."[44] This generally occurs during an intentional breach by maleficent actors, such as hackers[45] or as a result of a failure in operational security, or negligence, within an organization.[46] This distinction demonstrates how the rule set forth in *Clapper* should not be dispositive in regard to data breach cases.

II

Nevertheless, courts continue to use this "self-inflicted injury" reasoning found in *Clapper* to dismiss data breach cases for lack of standing. In the case of *In Re Zappos.com, Inc.*, a data breach exposed sensitive PII of nearly 24 million Zappos customers.[47] The plaintiffs sued, seeking damages stemming from an increased risk of identity theft and the cost to mitigate their increased risk of identity theft.[48] However, the court refused to hear the case on its merits, stating that "even when fears of future harm are not unfounded, plaintiffs simply cannot create standing by inflicting harm on themselves to ward off an otherwise speculative injury."[49] The court in *Zappos* reasoned that almost four years had passed since the Zappos.com data breach, but not a single plaintiff alleged actual identity theft or fraud. Therefore, the "Plaintiffs have not alleged a threat of future harm sufficiently imminent to confer standing."[50] According to the court in *Zappos*, "The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial."[51]

Similarly in *Reilly v. Ceridian Corp*, "an unknown hacker" caused a massive data breach that compromised the PII of "approximately 27,000 employees at 1,900 companies" whom used Ceridian for payroll services.[52] The sensitive PII exposed in *Reilly* included the full names, Social Security numbers, and

---

41. *See NSA Spying on Americans*, EFF, https://www.eff.org/nsa-spying (last visited Nov. 26, 2015) ("EFF is representing victims of the illegal surveillance program in *Jewel v. NSA*, a lawsuit filed in September 2008 seeking to stop the warrantless wiretapping and hold the government and government officials behind the program accountable.").

42. *See* Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html (Reporting on White House and Congressional leaders arguing that data collection is "necessary to protect national security.") (hereinafter *Online Data Overseas*).

43. Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 557 (2008), *available at* http://www.jetlaw.org/wp-content/journal-pdfs/Ciocchetti.pdf.

44. *Glossary of Privacy Terms*, INT'L ASS'N OF PRIVACY PROF'L, https://iapp.org/resources/glossary#data-breach (last visited Nov. 25, 2015).

45. *2015 Cost of Data Breach Study: United States*, PONEMON INST. 8 (May 2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF.

46. *Id.*

47. *In re Zappos.com* at *5.

48. *Id.*

49. *Id.* at *32 (citing *Clapper* at 1151) (internal quotation marks omitted).

50. *Id.* at *29.

51. *Id.* at *24-25.

52. *Reilly v. Ceridian Corp* at 40.

in some cases bank account information related to direct deposit accounts of the employees.[53] The plaintiffs brought suit against Ceridian alleging that as a result of the data breach, they were now at an increased risk of identity theft, and that they incurred costs to mitigate against the increased risk of identity theft.[54] In granting Ceridian's motion to dismiss, the Third Circuit Court of Appeals stated that allegations of future injuries "are not sufficient to satisfy Article III."[55] In support of their conclusion the Third Circuit held that the plaintiffs' claims are speculative, because their allegations rely on the hacker actually reading and understanding the stolen PII, and intending to misuse that information. The Third Circuit reasoned that, "[u]nless and until these conjectures come true, [plaintiffs] have not suffered any injury; there has been no misuse of the information, and thus, no harm."[56]

This is in stark contrast to *Remijas v. Neiman Marcus Group*.[57] In *Neiman Marcus*, the plaintiffs were 350,000 customers who had their credit card information along with other PII exposed following the breach of the Neiman Marcus customer database.[58] This data breach exposed more than 9,200 Neiman Marcus customers to fraud.[59] The trial court followed in the footsteps of *Clapper* by granting the defendant's motion to dismiss for lack of a "certainly impending" injury.[60] However, the Seventh Circuit Court of Appeals reversed, ruling that the ongoing risk to customers whose PII was compromised was sufficient to constitute an injury for the purposes of Article III standing.[61] The Seventh Circuit found that the plaintiffs, customers who were not yet aware of and unable to allege actual fraud, nonetheless faced a "substantial risk of future harm," and that substantial risk was sufficient to confer standing and to allow the denial of Neiman Marcus' motion to dismiss.[62]

ANALYSIS

The representative data breach cases cited above demonstrate the chaotic state of data breach litigation in the United States, resembling the beginnings of a circuit split.[63] The courts are split on the issue of whether a "substantial" increased risk of identity theft constitutes a sufficient, non-speculative injury for the purposes of Article III standing.[64] On one hand, some courts have used common sense in granting standing for victims of data

53. *Id*.
54. *Id.*
55. *Id.* at 42.
56. *Id.*
57. *Remijas v. Neiman Marcus Grp., LLC*, 2014 U.S. Dist. LEXIS 129574 (N.D. Ill. Sept. 16, 2014) (hereinafter "*Remijas I*").
58. *Id.* at *2.
59. *Id.*
60. *Id.*
61. *Remijas II* at 692.
62. *Id.*
63. *Katz v. Pershing* at 80; *see also* Supreme Court Rule 10(a) (Stating that Supreme Court review is appropriate when there is a circuit split. That is, when "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.").
64. *Id.* ("The courts of appeals have evidenced some disarray about the applicability of this sort of 'increased risk' theory in data privacy cases.").

breaches by recognizing the increased risk of identity theft.[65] And on the other hand, courts have used the decision in *Clapper*, a data collection case that is distinguishable from data breach cases, as the basis for denying standing on the grounds that an increased risk of identity theft is not enough.[66] In light of these considerations, it appears then that "a determination that a plaintiff lacks standing serves as a surrogate for disposition on the merits."[67] This outcome is wrong because data collection is not data breach, and the injury suffered following a data breach is sufficient enough to confer standing.

III

DATA COLLECTION IS NOT DATA BREACH

The standard set forth by *Clapper* is not appropriate for data breach cases because data breach cases are readily distinguishable from cases involving data collection. This distinction can be made in two ways. First, the facts of data collection cases are distinct from the facts in data breach cases. That is, in data breach cases there is generally a clear indication that PII has been accessed and exposed, whereas in a data collection case there is generally little indication either way. And second, in a typical data breach case the plaintiffs can rely on several strong arguments to effectively plead an actual injury – even if identity theft has yet to occur. On the contrary, with data collection cases it is generally difficult to determine whether a plaintiff has actually been injured because there is little indication data was accessed.

Facts In Each Case Are Distinguishable

The facts of *Clapper*, and data collection cases like it, are readily distinguished from the representative data breach case. In data collection cases, there is generally no clear indication whether that PII was actually accessed. For example, in cases like *Clapper*, the NSA does not eagerly admit to collecting information regarding the plaintiffs.[68] The majority in *Clapper* addresses this issue, finding that Amnesty International did not provide any indication as to whether the data was collected or not.[69] And in similar cases involving data collection for advertising and marketing purposes, the difficulty of determining if PII was actually collected or used is equally as difficult because the companies responsible for the data collection value the secrecy of their

---

65. *Remijas II* at 693 (Conferring standing for data breach plaintiffs, recognizing that "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

66. *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d. at 28 ("Indeed, since Clapper was handed down last year, courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases.").

67. Mark V. Tushnet, *New Law of Standing a Plea for Abandonment*, 62 CORNELL L. REV. 663, 699 (1977), *available at* http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4114&context=clr.

68. See generally *Clapper v. Amnesty*.

69. *Id.* at 1149 (2013)("Respondents, however, have set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted.").

practices.[70] On the contrary, in data breach cases, computer forensics experts can readily determine whether PII on a company's server was accessed, and the extent of the access, by reviewing the server access logs.[71] Further, a data collector can simply stop collecting data and the risk of harm is eliminated. For example, the harm of intercepted communications in *Clapper* would have ceased if the NSA ceased intercepting those communications. But unlike data collection, once a data breach is perpetrated the PII that is compromised can never be secured again.[72]

Additionally, a principled distinction can be made regarding the intentions of the data collector and the maleficent actor conducting a data breach. The motives of a data collector, usually a government or commercial advertising agency, are largely benign.[73] That is, data collectors are often only interested in collecting data for national security purposes[74] or for more effective marketing practices.[75] On the contrary, in a data breach cases, the motives are less likely to be benign. Hackers are generally interested in exploiting the data gathered for nefarious and illegal means, such as identity theft.[76] As such, it makes sense that a recent study sponsored by the National Consumers League suggests a strong correlation between identity theft and data breaches, with 66% to 82% of identity theft victims also being victims of data breaches.[77] And that correlation is made stronger when a Social Security number is exposed in a data breach, where data breach victims experience identity theft at a rate of 18 times the average.[78]

In sum, data breach and data collection are different. Their distinctions

---

70. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (Jun. 13, 2014), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. ("It's very hard to tell who is collecting or sharing your data—or what kinds of information companies are collecting.").

71. *See* Srinivas, *Log Analysis for Web Attacks: A Beginner's Guide*, INFOSEC INST. (Dec. 31, 2014), http://resources.infosecinstitute.com/log-analysis-web-attacks-beginners-guide/. ("[W]e will see how we can analyze the Apache server's access logs to figure out if there are any attacks being attempted on the website.").

72. Holly Andersen, Note, *A Website Owner's Practical Guide To The Wayback Machine*, 11 J. ON TELECOMM. & HIGH TECH. L. 251, 251 (2013) ("[…] the old adage that 'once on the Internet, always on the Internet' may ring true.").

73. *See generally* Ciocchetti, *supra* note 43.

74. *See, e.g.*, *Online Data Overseas*, *supra* note 42. (Reporting on White House and Congressional leaders arguing that data collection is "necessary to protect national security."); President's Review Grp. on Intelligence & Commc'n Tech., *Liberty and Security in a Changing World* 1 (2013) (emphasis added), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. ("[O]ur recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.").

75. *See* Ciocchetti, *supra* note 43 at 578-79. ("Sales of PII to unrelated parties provide an indirect benefit to consumers in the form of more efficient marketing.").

76. *See Antman v. Uber Technologies, Inc.*, 2015 U.S. Dist. LEXIS 141945, *28 (N.D. Cal. Oct. 19, 2015) ("The court thinks that a credible threat of immediate identity theft based on stolen data is sufficiently different than the speculative harm articulated in *Clapper*.") (citing *In re Adobe Systems Privacy Litig.,* 66 F. Supp. 3d 1197, 1215-16 (N.D. Cal. 2014) (noting the distinction between cases where a bad actor targets non-PII, such as a "GPS and stereo" and cases where stealing PII is the main objective of the bad actor)).

77. *See* NATIONAL CONSUMERS LEAGUE, *supra* note 77.

78. *See id.* at 14.

stem from the fact that there is a clear indication that hackers accessed PII in data breach cases, and the motives of the responsible parties are vastly different in each. As such, the standard for Article III standing set forth in *Clapper* should not be applicable to data breach cases.

Plaintiffs Have Suffered An Actual Present Injury After A Data Breach, Even If Identity Theft Has Yet To Occur

In *Ctr. for Law & Educ. v. Dep't of Educ.*, a suit challenging the composition of a negotiated rulemaking committee for the No Child Left Behind Act, the D.C. Circuit Court of Appeals noted, "were all purely speculative 'increased risks' deemed injurious, the entire requirement of 'actual or imminent injury' would be rendered moot, because all hypothesized, non-imminent 'injuries' could be dressed up as 'increased risk of future injury.'"[79] Essentially, the D.C. Circuit believed the plaintiffs were overstating the extent of their injury for the purposes of standing. However, that is not a concern that manifests itself in data breach litigation. Rather, as the true victims of the data breach, data breach plaintiffs do not need to dress up their injuries since the very compromise of their PII has caused the injury of an increased risk of identity theft. And even if actual identity theft has yet to occur, the specific maleficent intentions of a hacker[80] should be enough to demonstrate a cognizable injury that is sufficient to confer standing. This is because it is likely that, sooner or later, the hacker responsible for the breach will share or sell the stolen PII.[81] After which, identity theft is extremely likely to follow.[82] These plaintiffs are simply attempting to receive remuneration for their efforts in combating this increased likelihood of identity theft. Thus, there is a certainly impending and credible risk of harm, which causes people to take costly and inconvenient remedial measures in an attempt to avoid that harm.

In light of this risk of harm, the Seventh Circuit Court of Appeals,[83] in a recent data breach decision granting standing to data breach victims, rhetorically asked, "Why else would hackers break into a [company's] database and

---

79. *Ctr. for Law & Educ. v. Dep't of Educ.*, 396 F.3d 1152, 1161 (D.C. Cir. 2005).; *see also Baur v. Veneman*, 352 F.3d 625, 637 (2d Cir. 2003) (noting the "potentially expansive and nebulous nature of enhanced risk claims").

80. *See Antman v. Uber Technologies, Inc.*, 2015 U.S. Dist. at *28 ("The court thinks that a credible threat of immediate identity theft based on stolen data is sufficiently different than the speculative harm articulated in *Clapper*.") (citing *In re Adobe Systems Privacy Litig.,* 66 F. Supp. 3d. at 1215-16 (noting the distinction between cases where a bad actor targets non-PII, such as a "GPS and stereo" and cases where stealing PII is the main objective of the bad actor)).

81. Symantec Corp., *2015 Internet Security Threat Report*, 20 INTERNET SEC. THREAT REP. 1, 89 (2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

82. *See* NATIONAL CONSUMERS LEAGUE, CONSUMER DATA INSECURITY REPORT 10 (2014), *available at* http://www.nclnet.org/datainsecurity_report and http://www.javelinstrategy.com/uploads/web_brochure/TheConsumerDataInsecurityReport_byNCL.pdf. (link did not work)

83. *Remijas II* was not the first time the Seventh Circuit addressed this issue in a manner favorable to data breach plaintiffs. *See e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) ("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.").

steal consumers' private information?"[84] The Seventh Circuit provides the most plausible answer, "Presumably, the purpose of the [data breach] is, sooner or later, to make fraudulent charges or assume those consumers' identities."[85] The Seventh Circuit's answer is apt considering the hackers responsible for data breaches usually decide to sell the large troves of information they gather from data breaches on the black market.[86] For example, credit card information can sell for anywhere from $.50 to $20 per record.[87] And with most data breaches exposing an average of 3.2 million records,[88] there is a significant incentive for hackers to sell the PII they steal.[89] Not to mention, hackers that carry out data breaches submit themselves to civil exposure[90] and stiff criminal penalties.[91] Common sense, and a quick costs-benefits analysis, dictates that it would not make sense for a hacker to commit oneself to such enormous liability without a significant gain.

With these considerations in mind, it makes perfect sense why individuals perceive identity theft to be a credible threat following a data breach. And it also makes perfect sense why people feel compelled to expend time and money to take preventative measures to reduce their chances of falling victim to identity theft.[92]

The Court in *Clapper*, and its progeny, has considered these preventative or mitigating measures to be "self-inflicted injuries" for the purposes of standing.[93] Contrary to what the courts following this reasoning have held, the plaintiffs in data breach cases are not inflicting injury upon themselves in order to gain standing. Rather, the plaintiffs would presumably prefer to avoid facing this harm all together. But more importantly, the plaintiffs in data breach cases are responding to the serious, credible, and arguably overwhelming risk of identity theft brought upon them by the hacker's incentive to profit from the stolen PII. Ultimately, but for the data breach, the plaintiffs would not have incurred those costs or expended time attempting to guard themselves against the risk of identity theft. Therefore, any time and costs incurred by the plaintiffs in attempting to mitigate the increased risk of identity

---

84. *Remijas II* at 693.

85. *Id.*

86. Michael Riley, *Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar*, BLOOMBERG BUSINESS (Dec. 19, 2011), http://www.bloomberg.com/news/articles/2011-12-20/stolen-credit-cards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon ("How do cyber-bandits, who have turned hacking into a volume business, unload all those numbers? A lot like Amazon.com, it turns out.").

87. Symantec Corp., *supra* note 81.

88. *2015 Cyber Claims Study*, NETDILIGENCE 3 (Sept. 30, 2015), http://www.netdiligence.com/files/NetDiligence_2015_Cyber_Claims_Study_093015.pdf.

89. Symantec Corp., *supra* note 81.

90. *See* Corey Varma, *What is the Computer Fraud and Abuse Act (CFAA)?*, COREYVARMA.COM (Jan. 3, 2015), http://www.coreyvarma.com/2015/01/what-is-the-computer-fraud-and-abuse-act-cfaa/ (The CFAA "permits compensatory damages, injunctive and other equitable relief [.]").

91. 18 U.S.C. 1030(c) (2012); *see also* David J. Schmitt, *The Computer Fraud And Abuse Act Should Not Apply To The Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 425 (2014), *available at* https://dspace.creighton.edu/xmlui/bitstream/handle/10504/65317/47CreightonLRev423.pdf ("The CFAA has significant criminal sanctions[.]").

92. *See generally* ERIKA HARRELL, U.S. DEPARTMENT OF JUSTICE, VICTIMS OF IDENTITY THEFT 10 (2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

93. *Clapper* at 1152.

theft should appropriately be considered an injury for the purposes of an Article III standing analysis.

Alternatively, data breach plaintiffs have relied upon other theories to allege injury, including breach of implied contract and unjust enrichment.[94] As to the first, breach of implied contract, data breach plaintiffs will generally argue that contracting with a company in an exchange of money for goods or services, which incidentally requires the exchange of PII, includes the implied promise that the company will secure the PII and safeguard against data breaches.[95] This sort of implied contract is contemplated by the RESTATEMENT (SECOND) OF CONTRACTS. Section 4 of the RESTATEMENT (SECOND) OF CONTRACTS states, "A promise may be stated in words either oral or written, or may be inferred wholly or partly from conduct."[96] In the case of data breaches, the plaintiffs will usually ask the court to infer a promise to safeguard PII exchanged during a transaction. Some courts have found this theory convincing.

For example, *In re Hannaford Bros.*, customers filed suit against the Hannaford Brothers grocery chain alleging a breach of an implied contract following a massive data breach.[97] In *Hannaford* an unknown hacker or group of hackers infiltrated customer credit card information on a grocery store's computer system exposing approximately 4.2 million credit and debit card numbers and other customer PII.[98] The plaintiffs argued that the contract to purchase groceries included the implied promise to keep their PII safe.[99] The court in *Hannaford*, responding to the grocer's motion to dismiss, noted that whether there was an implied contract that Hannaford Brothers would "take reasonable measures to protect [their customers'] information" was a question of fact for a jury.[100] In making its decision, the court denied the defendant's motion to dismiss.[101] The *Hannaford* court reasoned that the contract to

---

94. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d at 1328 (11th Cir. 2012).

95. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.,* 613 F. Supp. 2d 108, 117 (D. Me. 2009).

96. RESTATEMENT (SECOND) OF CONTRACTS § 4 (1981); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 4 cmt. A (1981) ("Contracts are often spoken of as express or implied. The distinction involves, however, no difference in legal effect, but lies merely in the mode of manifesting assent. Just as assent may be manifested by words or other conduct, sometimes including silence, so intention to make a promise may be manifested in language or by implication from other circumstances, including course of dealing or usage of trade or course of performance.").

97. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.,* 613 F. Supp. 2d at 117.

98. *Id.*

99. *Id.* at 118 ("The plaintiffs assert that the merchant and consumer implicitly agree at the point of sale that the merchant will guaranty the consumer's electronic data against all intrusion.").

100. *Id.* at 119 ("If a consumer tenders a credit or debit card as payment, [the court] conclude[s] that a jury could find certain other implied terms in the grocery purchase contract: for example, that the merchant will not use the card data for other people's purchases, will not sell or give the data to others (except in completing the payment process), and will take reasonable measures to protect the information (which might include meeting industry standards), on the basis that these are implied commitments that are 'absolutely necessary to effectuate the contract,' and 'indispensable to effectuate the intention of the parties.'").

101. *Id.* ("[The court] conclude[s] that in a grocery transaction where a customer uses a debit or credit card, a jury could find that there is an implied contractual term that Hannaford will use reasonable care in its custody of the consumers' card data[.]"), *aff'd sub nom Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 158-59 (1st Cir. 2011) (finding that a jury must determine the existence of an implied contract term); *accord In re Target Corp. Customer Data Sec. Breach Litig.,* 66 F. Supp. 3d 1154, 1176-77 (D. Minn. 2014) ("As the In re Hannaford Bros. court found, a determina-

purchase goods required a payment by the customers, so a customer's use of a credit card could allow a jury to find certain other implied terms in the contract, such as taking reasonable measures to protect PII, on the basis that these are implied commitments that are "absolutely necessary to effectuate the contract" and "indispensable to effectuate the intention of the parties."[102] A plaintiff's reliance on the breach of implied contract theory of injury in a data breach case should thus be sufficient to confer standing and allow a trier of fact to hear the merits of the case.

As to the second theory of injury, unjust enrichment, according to a tentative draft of the RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT, "[a] person who is unjustly enriched at the expense of another is subject to liability in restitution."[103] Under the theory of unjust enrichment, data breach plaintiffs must first allege that they conferred a monetary benefit on a company.[104] That is, the plaintiffs paid the defendant-company for a good or service. Second, the data breach plaintiff must allege that the defendant-company appreciates the monetary benefit.[105] That is, the defendant-company appears to perform their end of the contract by executing its terms. Third, the plaintiffs must allege that the defendant-company uses the monetary benefit for the administrative costs of data management and security.[106] And finally, the plaintiffs must show that the defendant-company should not be permitted to retain the monetary benefit because the company failed to implement the promised data management and security measures.[107] In *Resnick v. AvMed, Inc.*, the Eleventh Circuit Court of Appeals found the plaintiffs' unjust enrichment argument to be convincing, allowing their claim to survive AvMed's motion to dismiss.[108]

In light of this, it seems that data breach plaintiffs are already armed with the means to claim a cognizable injury. But even with such a clear indication that the plaintiffs have suffered an injury, some courts are still generally reluctant to hear such cases on their merits. Rather, those courts still find the plaintiffs' injuries are too speculative to have standing.[109] As a consequence, the courts are split in regards to the increased risk of identity theft and the costs

---

tion of the terms of the alleged implied contract is a factual question that a jury must determine."); *see also In re Michaels Stores Pin Pad Litig.,* 830 F. Supp. 2d 518, 531-32 (N.D. Ill. 2011) ("[T]he allegations demonstrate the existence of an implicit contractual relationship between Plaintiffs and Michaels [.]").

102. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.,* 613 F. Supp. 2d. at 119.

103. RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (Tentative Draft No. 7, 2010).

104. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d at 1328.

105. *Id.*

106. *Id.*

107. *See, e.g.*, *Id.*

108. *Id.* ("Accepting these allegations as true, we find that Plaintiffs alleged sufficient facts to allow this claim to survive a motion to dismiss.").

109. *In re Zappos.com, Inc.*, 2015 U.S. Dist. LEXIS 71195, *25-26 (D. Nev. June 1, 2015) (citations omitted) ("The degree of Plaintiffs' speculation is heightened further by the fact that the future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor."); *In re Sci. Applications* at 26 ("[T]he Third Circuit held that, where it was 'not known whether the hacker read, copied, or understood the data,' injury remained speculative."); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012) ("Most courts have held that such plaintiffs lack standing because the harm is too speculative."); *see also Clapper* at 1149-50 (refusing to grant standing based on speculation).

to mitigate the increased risk of identity theft theories of injury. This creates a vacuous arena for data breach litigation that leads to potentially unfavorable outcomes. The proposal set forth in the next section provides courts with a cogent and uniform standard to cope with data breach litigation.

IV

PARADIGM SHIFT: CHANGING THE WAY WE THINK ABOUT STANDING IN DATA BREACH CASES

In order to permit plaintiffs to argue their case on its merits, this comment proposes a standard that presumes an injury in favor of plaintiffs in a case of data breach. That is, where the plaintiffs can allege facts that an unidentified maleficent actor has gained access to their PII through potentially unlawful means, there should be a strong presumption that the PII accessed will be used for nefarious and fraudulent purposes. This allows data breach plaintiffs to satisfy the injury requirement for standing, which allows the plaintiffs to argue their case on its merits.

Such a presumption of injury is justiciable because courts have granted standing in cases with more tenuous injuries. Additionally, this presumption of injury is fair because it allows defendant companies to rebut the presumption with evidence that the alleged injury is not imminent. And finally, this presumption of injury encourages businesses to take data breaches seriously by exposing them to liability for failure to take reasonably necessary steps to secure their customers PII.

The Presumption Of Injury-In-Fact Is Justiciable

The presumption of injury in data breach cases is justiciable because courts have found Article III standing to be appropriate in cases where the plaintiffs' injuries are far more tenuous, transcending "economic and physical interests," such as when "aesthetic, spiritual, and recreational interests" are at stake.[110] Further, the presumption of injury is justiciable because the dissent in *Clapper*, written by Justice Breyer, recognizes that "courts have often found probabilistic injuries sufficient to support standing."[111]

Courts have broadened the injury requirement for standing to encompass injuries that are imminent: that is, they have yet to occur, but are certain to occur.[112] This alone would seem to support the idea that standing is appropriate for data breach plaintiffs because misuse of their PII seems certain. Nonetheless, in his dissent in *Clapper*, Justice Breyer contends that "certainty is not,

---

110. F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 65 n.51 (2012) (citing *Association of Data Processing Service Organizations, Inc. v. Camp*, 397 U.S. 150, 154 (1970) (emphasizing that standing "may stem from [non-economic injuries]" as well as economic injuries)).

111. *Clapper* at 1161 (Breyer, J., dissenting) ("courts have often found probabilistic injuries sufficient to support standing.").

112. Hessick, *supra* note 110 at 65 (citing *Regional Rail Reorganization Act Cases*, 419 U.S. 102, 143 (1974) ("If an injury is inevitable, it is justiciable even if it may not occur until the distant future.")).

and never has been, the touchstone of standing."[113] In support of this proposition, Justice Breyer poses a *reductio ad absurdum*[114] hypothetical situation where "a federal court faced a claim by homeowners that (allegedly) unlawful dam-building practices created a high risk that their homes would be flooded."[115] Justice Breyer contemplates whether the Court "deny [the plaintiffs] standing on the ground that the risk of flood was only 60, rather than 90, percent."[116] The point being: where do we draw the line? If "certainly impending" is important, then how is it quantified? And at what degree is a threatened injury "certainly impending" for the purposes of standing?

The majority of the Court in *Clapper* concedes that imminence is "a somewhat elastic concept," limiting imminence to "certainly impending" injuries.[117] Even under this higher standard of "certainly impending," data breach plaintiffs should still be entitled to standing because, when PII is compromised in a data breach, as discussed in the previous section, the threat of becoming a victim of identity theft is more than certainly impending, it is almost inevitable. Because the threatened injury of identity theft following a data breach is almost inevitable, standing is appropriate "even if [the harm] may not occur until the distant future."[118]

Further, Justice Breyer explains in his dissent that the Court has found standing appropriate for "plaintiffs [that] would suffer present harm by trying to combat the [future] threat."[119] This is precisely what data breach plaintiffs allege when they endeavor to combat the actual future threat of identity theft, a real harm that is rooted in their reasonable fear that hackers may misuse their PII. And, but for the data breach, the plaintiffs would not be faced with the onerous task of monitoring their credit and otherwise attempting to avoid identity theft. As a result, these data breach plaintiffs not only suffer the possibility of future harm, but also suffer a present harm by expending time and money to mitigate that threat of the future harm.

Rebuttable: Companies Can Still Argue That There Is No Injury-In-Fact

Under this proposal, once the data breach plaintiffs allege injury through an increased risk of harm, the court should presume their injury for purposes of standing. However, in the spirit of fairness, the defendant should have the opportunity to rebut the presumption of injury with evidence of several mitigating factors that may support a motion to dismiss. The strongest argument a data breach defendant could make is that no PII was actually taken, or that the

113. *Clapper* at 1160 (Breyer, J., dissenting).

114. Nicholas Rescher, *Reductio ad absurdum*, INTERNET ENCYCLOPEDIA OF PHILOSOPHY, http://www.iep.utm.edu/reductio/ (last visited July 21, 2009) ("In its most general construal, *reductio ad absurdum* […] is a process of refutation on grounds that absurd – and patently untenable consequences would ensue from accepting the item at issue.").

115. *Clapper* at 1162-63 (Breyer, J., dissenting).

116. *Id.* at 1162-63 (Breyer, J., dissenting).

117. *Id.* at 1147 (citing *Lujan v. Defenders of Wildlife* at 557 (1992) (Recognizing imminence to be "a somewhat elastic concept")).

118. Hessick, *supra* note 110 at 65 (2012) (citing *Regional Rail Reorganization Act Cases*, 419 U.S. 102, 143 (1974)).

119. *Clapper* at 1164 (Breyer, J., dissenting) (citing *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010)).

stolen PII was encrypted (and effectively indecipherable to the hackers[120]), meaning that potentially no injury could occur.

In keeping with the strong presumption of injury in these cases, the court's reasoning should be guided by all the facts and circumstances surrounding the data breach. Additionally, the court should consider whether evidentiary support is given to the arguments made by the defendant company. For example, if a company contends that no injury could potentially result because the stolen PII was encrypted, the court should require the company to lend evidentiary support to their assertion that the encryption met or exceeded industry standards for the type of data that was stolen.[121]

Public Policy: Encourages Companies To Take Security Of PII Seriously

The average cost of a data breach to a company in 2014 was $6.5 million dollars.[122] In the same year, there were 783 data breaches.[123] But data breaches continue to occur and with even more frequency, while companies have seemingly failed to take reasonable steps to secure sensitive PII. Taking data security seriously is a necessity in today's interconnected world. The proposal outlined in this comment attempts to encourage businesses to take data security seriously.

By permitting plaintiffs to have standing, businesses will be held accountable for their failure to secure PII through the potential for liability. This potential liability should encourage businesses to take meaningful steps to secure PII. Consequently, reducing the overall costs of data breaches, both the financial costs to the business and costs to individuals. If courts continue to refuse to confer standing, there will be little incentive for businesses to use reasonable methods to secure customer PII, which sends the wrong message to businesses. On the contrary, permitting plaintiffs to have standing in data breach cases ensures accountability for insufficient data security and stimulates businesses to take affirmative steps to secure their customers PII, thereby reducing the overall costs of data breaches.

V

HYPOTHETICAL EXAMPLE: THE APPLICATION OF THE PRESUMPTION OF INJURY FOLLOWING A DATA BREACH

As an example of the application of the proposal outlined in this comment, consider a hacker or group of hackers manages to infiltrate the servers

120. Symantec Corp., *supra* note 81 at 104 (Symantec recommends that businesses encrypt customer data because encryption "serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization."); *see also* 2 ODED GOLDREICH, FOUNDATIONS OF CRYPTOGRAPHY: BASIC APPLICATIONS 374 (2004).

121. *See generally*, Nat'l Inst. Sci. Tech., *Federal Information Processing Standards Publication 197: Announcing The Advanced Encryption Standard (AES)*, FIPS PUBS (Nov. 26, 2001), *available at* http://www.nist.gov/itl/upload/fips-197.pdf and http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

122. *2015 Cost of Data*, *supra* note 45 at 1.

123. *Identity Theft Resource*, *supra* note 2.

of a large online business. Pretend this online business is a paid online dating service that caters to people who are either married or in a committed relationship, but are also interested in infidelity.[124] As a result of this data breach, a horde of data was exposed. Much of the data and PII exposed in the data breach were customer records, including the real names of the adulterous dating service's customers, credit card details, billing addresses, and sexual fantasies, among other information.[125] And as a result of the data breach, the plaintiffs have purchased credit monitoring to guard against identity theft.

Understandably upset, and presumably embarrassed, the customers of the paid dating service file suit in Federal Court under class action diversity jurisdiction against the company alleging: the breach of an implied contract to keep their PII secure, and unjust enrichment for taking money for a service that was substandard (among other claims, such as intentional infliction of emotional distress). The principal injury the plaintiffs rely upon for the purposes of Article III standing is the theory that the data breach has put the plaintiffs at an increased risk of identity theft. Further, the plaintiffs also allege a present injury of expending time and money for credit monitoring in an attempt to guard against the future harm of identity theft.

Under the current circuit split, where the plaintiffs bring suit will be outcome determinative. It is likely, based on the outlay of the courts, that the suit will be dismissed out of hand, before the case reaches the merits stage, because the courts have not universally accepted the increased risk of identity theft theory of injury. If the plaintiffs in this hypothetical situation bring their suit in the Seventh Circuit, relying on *Remijas*, there is a high likelihood that they will be able to demonstrate an injury under the increased risk of identity theft theory. But in the Third Circuit, based on the ruling in *Reilly*, the court will likely dismiss the case for lack of a concrete and particularized injury.

However, per the proposal outlined in this comment, the court would deny the defendant's motion to dismiss for lack of standing. Rather the court would presume an injury that would allow the plaintiffs to survive the motion to dismiss and argue the case on its merits. To obtain this presumption, the plaintiffs would first allege that an unidentified maleficent actor (a hacker) has gained access to customer PII on the defendant's servers. With this in mind, the court should consider both the type of PII that was accessed, and the hacker's intentions in accessing that PII. The court should assume that the hackers are likely interested in profiting from the data breach and the stolen PII by selling it on the black market, subjecting the plaintiffs to the remarkably high risk of identity theft. Accordingly, the court will presume that the PII accessed or stolen will be used for nefarious purposes. This establishes a concrete and particularized, imminent injury. And the court will appropriately regard any time and money spent in combatting this high risk of injury as a present injury. This injury would, at the very least, be sufficient to deny the

---

124. Forgetting about any possible jurisdictional issues that might come up in filing suit against AshleyMadison, a website operated by Avid Life Media, which is a Toronto, Canada based company. *See generally* Brian Krebs, *Online Cheating Site AshleyMadison Hacked*, KREBS ON SEC. (July 19, 2015), https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

125. *Id.*

defendant company's motion to dismiss so that the case can be heard on its merits.

CONCLUSION

With the proliferation of technology in our society, and the unrelenting adoption of technology in business transactions, comes an inherent responsibility to guard PII. And when a business fails to guard their customers' PII and suffers a data breach, that company has the responsibility to redress both the present and future injuries their customers face as a result of the data breach; the present injury of having to expend time and money in guarding against the very real possibility of identity theft, and the future injury of identity theft. Both injuries are sufficient to confer standing. The true victims of data breaches should not be turned away at the courthouse steps. Rather, they should be allowed to argue their case on the merits.

The proposal set forth in this comment gives courts a cogent means of conferring standing when a plaintiff has alleged the present injury of expending time and money in the hopes of warding off the future injury of identity theft that follows a data breach. By presuming that those plaintiffs have suffered an injury through the overwhelming risk of imminent identity theft following a data breach, courts can finally reconcile the harsh realities of today's interconnected world. At the same time, this proposal contemplates due process and fairness to the defendant by allowing them to rebut the presumption with evidence that the data breach could not foreseeably result in an injury. Conferring Article III standing in this manner allows these plaintiffs to argue their case on its merits, allowing the true victims of data breaches to seek redress for the costs and inconvenience of data breaches. Moreover, this proposal enriches public policy by opening up liability to businesses that have failed to reasonably secure their customers' PII. This encourages businesses to make the secure collection, storage, and use of PII a priority, which reduces the overall societal costs of data breaches.

As technology continues to proliferate our society and information security becomes more important to consumers, the courts will take notice. And as information security takes center stage, the question of standing for the true victims of data breach will become painfully obvious. The sooner that day comes, the better.