Hastings Law Journal

Volume 69 | Issue 2 Article 6

2-2018

No Harm, Still Foul: When an Injury-in-fact Materializes in a Consumer Data Breach

Benjamin C. West

No Harm, Still Foul: When an Injury-in-fact Materializes in a Consumer Data Breach

BENJAMIN C. WEST*

In the consumer data breach context, courts have seemingly limited a plaintiff's ability to bring suit by applying the standing doctrine's injury-in-fact requirement too rigidly. This is unacceptable, as the law of standing should not leave consumers without technology, without security, and without recourse. This Note challenges how courts currently apply the injury-in-fact element in consumer data breach actions, and proposes a new standard that better understands and considers previously overlooked harms that are incurred upon a breach.

This Note proceeds in four parts. Part I describes how courts currently approach standing in consumer data breach actions. Part II illuminates a plethora of real harms that current approaches fail to consider. Part III addresses foreseeable counterarguments. Lastly, Part IV urges courts to consider reforming current approaches by stressing how a better understanding of what constitutes a sufficient harm will ultimately provide adequate recourse to harmed consumers.

* J.D. Candidate 2018, University of California, Hastings College of the Law; B.A. 2013, University of California, Irvine. I want to thank Professor Scott Dodson for introducing me to the area of law that inspired this Note, and for his invaluable feedback and suggestions. I dedicate this Note to my mother, Deborah West. This Note would not have been possible without her unconditional love and support.

TABLE OF CONTENTS

INTRODUCTION

Despite the valiant efforts of many of our parents and grandparents to resist technological advancements, it is safe to say that technology has carried the day. Thirty years ago, phones were the size of bricks, record stores were still profitable, online-dating did not exist, and people still had to leave the house to buy groceries. Today is quite different. As an example, the phone currently in your pocket is more technologically powerful than every single NASA computer used to get Neil Armstrong to the moon.[1]

Technologic advancement comes with both benefits and new risks of harm. Technology is part of everything we do now. Personal information appears throughout emails, social media pages, and texts. Scores of businesses maintain your credit or debit card information. Whether you ordered a pizza online last week, bought new socks off of Amazon, or decided to take an Uber into work this morning, chances are, the information stored securely in your wallet is not as secure as you think.

The biggest risk to stored consumer information is a data breach. As the Third Circuit said, arguably with only modest overstatement, "[t]here are only two types of companies left in the United States, according to data security experts: 'those that have been hacked and those that [do

1. Tibi Puiu, *Your Smartphone Is Millions of Times More Powerful than All of NASA's Combined Computing in 1969* (Sept. 10, 2017, 1:53 PM), ZME SCI., www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432.

not] know [they have] been hacked.'"[2] In fact, in 2014, it was reported that as many as "43% of companies have experienced a data breach . . . . Even worse, the absolute size of the breaches [has been] increasing exponentially."[3] Recent statistics have found that individuals who have been the victim of a data breach are nine and a half times more likely to become the victim of identity theft.[4]

When a data breach occurs, various laws provide consumers with the ability to seek redress against the companies that failed to protect their information. However, recent cases have limited a plaintiff's ability to bring suit in federal court by rigidly applying the standing doctrine's injury-in-fact requirement to consumer data breach suits.

Though the United States Supreme Court announced in *Clapper v. Amnesty International USA* that allegations of potential harm must be "certainly impending" to state a justiciable case,[5] this standard severely understates certain real harms attributable to data breaches. In 2016, the Supreme Court in *Spokeo, Inc. v. Robins* had a chance to remedy the nearsightedness of *Clapper*, but the Court avoided deciding the issue entirely.[6]

The purpose of this Note is not to attack the standing doctrine, but rather to challenge how some courts currently apply the injury-in-fact element in consumer data breach suits. This Note urges a different understanding of injury-in-fact in relation to consumer data breach cases: one that recognizes the real financial risks and psychological harms to consumers. Specifically, the injury-in-fact requirement should be applied with the understanding that a breach in and of itself is an actual harm to consumers who are currently forced to use technology without sufficient protection. This standard will allow consumers who are harmed in less tangible and physical ways to have opportunities to seek redress. In the case of a data breach, the law of standing ought not leave consumers without technology, without security, and without recourse.

This Note defends its proposed thesis in four parts. Part I describes how courts currently approach standing in consumer data breach suits. Part II illuminates a plethora of very real harms that these current approaches fail to consider. Part III addresses foreseeable

2. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015) (quoting Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES (Apr. 22, 2013, 9:10 PM), http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=0).

3. *Storm*, 90 F. Supp. 3d at 360–61 (citing Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197).

4. *Identity Shield—Identity Theft Statistics*, STARR WRIGHT USA, http://test.wrightusa.com/products/wright-identity-shield/statistics (last visited Jan. 20, 2018).

5. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

6. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1553 (2016).

counterarguments. Lastly, Part IV urges courts to consider reforming current approaches to the injury-in-fact element of standing as it relates to consumer data breach cases. The Note concludes by stressing how a better understanding of what constitutes a sufficient harm in consumer data breach suits will ultimately provide adequate recourse to harmed consumers.

I. THE CURRENT APPROACH TO STANDING IN CONSUMER DATA BREACH SUITS

A. THE ROAD TO *CLAPPER*

Article III, Section 2 of the United States Constitution authorizes federal courts to adjudicate only actual "cases" and "controversies."[7] The Supreme Court has interpreted these words as prescribing judicial limitations on the types of cases that can be brought before a court. The standing doctrine is the most notable of these limits. Standing has been understood as the determination of whether a specific person is the proper party to bring a matter to the court for adjudication.[8] "Current standing doctrine purports to ask . . . whether plaintiffs have an adequate stake in seeking judicial relief."[9] Standing prohibits courts from issuing advisory opinions and from hearing moot or unripe cases.[10]

A plaintiff must show three elements to have standing.[11] First, a plaintiff must have suffered an actual injury.[12] Second, a plaintiff must allege that the injury is fairly traceable to the defendant's conduct.[13] Third, a plaintiff must allege that a favorable court decision is likely to redress the injury.[14] Importantly, the burden is on the plaintiff to satisfy these elements.[15]

The most prominent issue of standing, as applied to consumer data breach cases, concerns the injury element. A standing injury requires "an invasion of a legally protected interest which is (a) concrete and

7. U.S. CONST. art. III, § 2.

8. *See* Allen v. Wright, 468 U.S. 737, 750–51 (1984) (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)) ("In essence the question of standing is whether [a] litigant is entitled to have [a] court decide the merits of the dispute or of particular issues." (internal quotations omitted)).

9. Richard M. Re, *Relative Standing*, 102 GEO. L.J. 1191, 1191 (2014).

10. Evan Tsen Lee, *Deconstitutionalizing Justiciability: The Example of Mootness*, 105 HARV. L. REV. 605, 606 (1992).

11. This Note only addresses the standing doctrine's constitutional requirements, and does not discuss any potential prudential requirements.

12. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

13. *Lujan*, 504 U.S. at 590 (Blackmun, J., dissenting).

14. *Id.* at 561.

15. *See id.* at 566 (quoting United States v. Students Challenging Regulatory Agency Procedures ("SCRAP"), 412 U.S. 669, 688 (1973)) ("Standing is not 'an ingenious academic exercise in the conceivable,' but [instead] requires . . . a factual showing of perceptible harm.").

particularized . . . and (b) actual or imminent."[16] A plaintiff's alleged injury "must be . . . distinct and palpable, and not abstract or conjectural or hypothetical."[17] More specifically, most courts grapple with the issue of whether an alleged risk of future harm caused by a data breach is a sufficient injury-in-fact. A majority of courts have held that where a plaintiff fails to allege an injury that is either "actual or imminent," there is no standing under Article III.[18] Nevertheless, a number of "courts . . . have held that the injury-in-fact requirement can be satisfied by a threat of future harm or by any act that harms plaintiff only by increasing the risk of future harm that plaintiff would have otherwise faced, absent defendant's actions."[19] A notable example of this is illustrated by *Massachusetts v. EPA*, where the Supreme Court held that Massachusetts—as well as other states—had suffered a sufficient injury-in-fact in order to proceed in a suit against the Environmental Protection Agency ("EPA") for failing to regulate carbon dioxide and other greenhouse gases as pollutants.[20] In holding that plaintiffs had standing, the Court stressed that "the rise in sea levels associated with global warming has already harmed and will continue to harm [states]. The risk of catastrophic harm, though remote, is nevertheless real."[21]

The Supreme Court's prominent *Clapper* opinion addressed what kind of future harm satisfies the injury-in-fact element of standing in relation to government surveillance suits.[22] In *Clapper*, attorneys and human rights, labor, legal, and media organizations challenged section 702 of the Foreign Intelligence Surveillance Act, which authorized governmental surveillance of non-U.S. persons "reasonably believed to be located outside of the United States."[23] In asserting that Article III standing was met, the plaintiffs argued that the nature of their work "require[d] them to engage in sensitive international communications with . . . likely targets" of the Act, and that there was an "objectively reasonable likelihood that their communications [would] be acquired . . . at some point in the future."[24] The Court rejected this argument, stressing that there was no evidence that plaintiffs had been placed under surveillance and the fact that plaintiffs could be surveilled at some point in the future was insufficient.[25] The Court maintained that

16. *Id.* at 560 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)) (internal quotations omitted).

17. Allen v. Wright, 468 U.S. 737, 751 (1984) (citation and internal quotations omitted).

18. *Lujan*, 504 U.S. at 560.

19. DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 31.03 (Matthew Bender ed., rev. ed. 2017).

20. Massachusetts v. Envtl. Prot. Agency, 549 U.S. 497, 498 (2007).

21. *Id.* at 526.

22. Clapper v. Amnesty Int'l, USA, 133 S. Ct. 1138, 1142 (2013).

23. *Id.* (citing 50 U.S.C. § 1881a (2006)).

24. *Clapper*, 133 S. Ct. at 1142.

25. *Id.* at 1148.

plaintiffs' theory of future injury was "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending."[26] The Court held that allegations of future harm can only establish Article III standing if the alleged harm is "certainly impending."[27] For the Court, "allegations of *possible* future injury are not sufficient."[28]

The plaintiffs in *Clapper* alternatively argued that they had suffered present injury because the risk of surveillance had already "forced them to take costly and burdensome measures to protect the confidentiality of their international communications."[29] In rejecting this argument, the Supreme Court held that plaintiffs could not "manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[30]

The Supreme Court has not yet explained how far *Clapper* extends. In *Spokeo*, a Virginia man named Thomas Robins ("plaintiff") brought suit against a "people search engine" company (Spokeo), when the company published false information about him.[31] The false information indicated that plaintiff was wealthy, married with children, and worked in a professional or technical field.[32] In fact, plaintiff was not married, did not have children, and was unemployed and looking for work.[33] The issue before the Court was whether a plaintiff has standing when a web company posts incorrect information about him, where the harm has yet to materialize. The Court did not answer that question but instead, in a 6-2 decision, concluded that the Ninth Circuit had failed to consider standing fully.[34] The Court remanded the case to allow the Ninth Circuit to apply the injury-in-fact requirement in the first instance.[35] However, in her dissent, Justice Ginsburg stated that the plaintiff had alleged a sufficient injury-in-fact because Spokeo's misrepresentation of personal details had harmed plaintiff's job prospects.[36]

B. *CLAPPER* APPLIED

Although *Clapper* was not a consumer data breach case, courts have applied the *Clapper* standard to consumer data breach suits.[37] For

26. *Id.* at 1143.
27. *Id.*
28. *Id.* at 1147 n. 9.
29. *Id.* at 1143.
30. *Id.*
31. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016).
32. *Id.* at 1546.
33. *Id.*
34. *Id.* at 1553.
35. *Id.* at 1554.
36. *Id.* at 1555 (Ginsburg, J., dissenting).
37. Both the Second and Fourth Circuits have relied on *Clapper* in finding allegations of increased risk of harm insufficient to confer standing. *See* King & Spalding, *D.C. Circuit Revives Data Breach*

example, in *Whalen v. Michaels Stores Inc.*, a trial court in the Second District followed *Clapper* in finding a lack of standing in a suit where customers alleged an increased risk of future harm.[38] There, Michaels notified customers of "possible fraudulent activity" on some of Michaels' customers' credit cards whose data Michaels kept and maintained.[39] Three months later, Michaels confirmed the existence of a security breach.[40] According to the company's press release, hackers used malicious software to retrieve the credit card information from the systems of Michaels stores and its subsidiary, Aaron Brothers.[41] Michaels estimated that approximately 2.6 million credit or debit cards may have been affected during the time period of the alleged breach.[42] Whalen alleged that she had suffered damages arising out of "costs associated with identity theft and the increased risk of identity theft," namely, lost time and money associated with credit monitoring and other risk-mitigation efforts, though she conceded that "fraudulent use of cards might not be apparent for years."[43]

Applying *Clapper*, the court rejected Whalen's argument and held that she lacked standing, reasoning that plaintiffs "cannot manufacture standing" through credit monitoring.[44] The court maintained that "[i]f 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."[45]

Similarly, in *Storm v. Paytime, Inc.*, a district court judge found a lack of standing based on *Clapper*'s "certainly impending" standard in a class action suit against a payroll service company.[46] There, a data breach exposed employees' confidential personal and financial information, including full legal names, addresses, bank-account information, social security numbers, and dates of birth.[47] Although the breach occurred on April 7, 2014, the defendant did not discover the breach until April 30, 2014.[48] Moreover, the defendant waited until May 12, 2014 to begin notifying affected employers of the breach.[49] The plaintiffs in *Storm* claimed "that nationally, over 233,000 individuals had their personal

---

Putative Class Action on Standing Grounds, Widens Circuit Split, JD SUPRA (Aug. 22, 2017), www.jdsupra.com/legalnews/d-c-circuit-revives-data-breach-78728.

38. Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015).
39. *Id.* at 578.
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.* at 579.
44. *Id.* at 581.
45. *Id.*
46. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 364 (M.D. Pa. 2015).
47. *Id.* at 363.
48. *Id.*
49. *Id.*

and financial information 'misappropriated' as a result of the breach of [defendant's] computer network."[50] They brought suit alleging that as a result of the data breach, "they . . . have spent, or will need to spend, time and money to protect themselves from identity theft."[51]

The plaintiffs also asserted present damages.[52] One class member—a government employee who needed security clearance to perform his job—had his security clearance suspended as a result of the breach and was required to work at a different job site which resulted in a four hour increase in his daily commute.[53] He alleged that the increased commute caused him to incur travel expenses and lost time.[54]

In dismissing the suit for lack of standing, the court embraced *Clapper* by finding "no factual allegation of misuse or that such misuse is certainly impending."[55] The court found that plaintiffs did not allege that their bank accounts had been accessed, that credit cards had been opened in their names, or that unknown third parties had used their social security numbers to impersonate them and gain access to their accounts.[56] "In sum, their credit information and bank accounts look the same today as they did prior to [defendant's] data breach."[57]

Many courts have agreed that, following *Clapper*, increased risk alone cannot meet the injury-in-fact requirement in consumer data breach cases because the harm is "merely speculative."[58] However, some courts have approached the issue differently.[59] Notably, the Seventh Circuit, in *In re Adobe Systems Privacy Litigation*, distinguished *Clapper* in a consumer data breach suit and refused to apply its "certainly impending" standard.[60] "Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,'" the court found that "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real."[61]

Similarly, in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit again distinguished the harms alleged in *Clapper* from the harms

50. *Id.*
51. *Id.*
52. *Id.* at 364.
53. *Id.*
54. *Id.*
55. *Id.* at 366.
56. *Id.*
57. *Id.*
58. *See, e.g.*, Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871 (N.D. Ill. 2014) (*Clapper* compels rejection of [plaintiff's] claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing.").
59. The Sixth, Seventh, Ninth and D.C. Circuits have all held that increased risk of harm is sufficient for standing purposes. King & Spalding, *supra* note 37.
60. *In re* Adobe Sys., Inc. Privacy Litigation, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).
61. *Id.* at 1214.

alleged in a consumer data breach suit.[62] In *Remijas*, 350,000 account cards were potentially exposed to malicious malware that infiltrated Neiman Marcus's computer systems.[63] Over 9000 of those cards were then used fraudulently.[64] In finding that those consumers who had alleged only imminent future injuries had standing, the court emphasized that plaintiffs in a data theft case are differently situated from the plaintiffs in *Clapper*.[65] In particular, the victims of the Neiman Marcus data breach did not "need to speculate as to whether [their] information [had] been stolen . . . ."[66] Both parties agreed that the information had been taken, and for the court, this was sufficient.[67] The court found that "[defendant's] customers should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[68] The court stated that "[p]resumably, the purpose of the hack [was], sooner or later, to make fraudulent charges or [to] assume [plaintiffs'] identities."[69] In maintaining that there was an "objectively reasonable likelihood" that identity theft would occur to all consumers involved in the consumer data breach, the court rhetorically asked: "Why else would hackers break into a store's database and steal consumers' private information?"[70] Given this important notion, the court found that plaintiffs' "allegations of future injury are sufficient" to establish standing.[71]

Other courts have found that allegations of a substantial risk of harm, along with reasonably incurred mitigation costs following a data breach, are sufficient to establish a cognizable injury and confer standing under Article III. For example, in *Galaria v. Nationwide Mutual Insurance Co.*, the Sixth Circuit found that various costs (in both time and money) commonly incurred by victims of identity theft and fraud are sufficient to satisfy the injury-in-fact standing requirement.[72] The court there stated that "[w]here [p]laintiffs already know that they have lost control of their data, it would be unreasonable to expect [them] to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial

62. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).
63. *Id.* at 690.
64. *Id.*
65. *Id.* at 693.
66. *Id.*
67. *Id.*
68. *Id.* (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).
69. *Remijas*, 794 F.3d at 693.
70. *Id.*
71. *Id.* at 694.
72. Galaria v. Nationwide Mutual Ins. Co., Nos. 15-3386/3387, 2016 U.S. App. LEXIS 16840, at *9 (6th Cir. Sep. 12, 2016).

security."[73] For the court, "these [preventative] costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing."[74]

II. RETHINKING INJURY IN CONSUMER DATA-BREACH SUITS

Neither the majority nor the minority position has it completely right. Both camps fail to appreciate that consumer data breach victims suffer both a credible risk of future injury and a concrete present injury, and that these injuries are sufficient to confer standing, even under *Clapper*.

Clapper drew a distinction between "certainly impending" and merely "possible" future harm. Critically, though *Clapper* was a government surveillance case, there was no allegation that the plaintiffs were under surveillance.[75] The plaintiffs argued that the type of work they engaged in made it objectively reasonable that their communications would eventually be subject to government surveillance, but the Court concluded that the likelihood of surveillance was "too speculative" to be considered an actual harm under the standing doctrine.[76] Further, there was no concrete present injury in *Clapper*, but the Court stated that actual unlawful surveillance alone would have been a sufficient harm.[77]

In the consumer data breach context, by contrast, possible risk of harm is not speculative. When a consumer data breach occurs, it means that someone has deliberately taken consumer information for misuse. Breaches do not occur randomly. Data thieves steal information to use it. Even if the stolen data is not used for a number of years—or even if it is not used at all—this does not discount the fact that private information is in the wrong hands and consumers are forced to live with a heightened risk of identity theft.

Further, consumer data breach victims suffer actual *present* harm. Unlike the plaintiffs in *Clapper*, who had not yet been surveilled, a data breach victim's privacy has been breached. Victims of a data breach suffer several present injuries, including financial loss associated with attempts to mitigate the risk of identity theft, lost time, and psychological harms that arise from the breach itself.

A. FUTURE RISK OF INJURY

No one questions whether respondents' communications in *Clapper* would have been surveilled at some point, given that respondents were lawyers and rights organizations who spoke regularly to persons the Act

73. *Id.* at *10.
74. *Id.* at *11.
75. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1141 (2013).
76. *Id.* at 1143.
77. *Id.* at 1153.

was created to target. As such, *Clapper* arguably was wrongly decided. However, even if *Clapper* was correctly decided, the "certainly impending" standard is misapplied in the consumer data breach context because its application severely understates very real harms. In a consumer data breach suit, a breach has occurred. Private information is no longer secure. It is no longer in the hands of the entities charged with protecting it. Instead, it is in the hands of people who ultimately plan to use it for personal gain. As such, a future risk of harm ceases to be speculative once there has been a data breach. Once a breach occurs, there is an objectively reasonable likelihood that the information has or will ultimately end up in the wrong person's hands.

That the risk may be small does not make it too speculative to confer standing, either. The degree of risk will likely be considered in determining proper damages; however, even a small risk of identity theft should constitute actual harm for standing purposes. Any heightened risk creates a fear that is objectively reasonable. The fact that consumers may never suffer financial harm does not discount the fact that consumers will undoubtedly respond to the heightened risk in ways that reflect sufficient actual harms. Critics could rightfully argue that the risk is still a question of whether, not when, consumers will incur non-financial harms resulting from consumer data breach. However, Subpart B of this Part importantly shows that there are property and privacy rights that presume actual harm as soon as a breach occurs, regardless of whether the data is fraudulently used.

Further, *Clapper*'s "certainly impending" standard cannot exclude a data breach risk of future harm just because the risk is long-term. A risk that was not present before is a harm. As such, long-term risk is still an actual harm. Unlike a claim against a thief for future misuse, here, companies are data-confidants who breached their duty to keep private information secure. Consumers do not really have a choice in releasing their private information to companies. As such, the injury caused by the failures of companies to protect confidential information is ripe immediately upon a data breach. Just like business partners can be jointly and severally liable,[78] here too the companies do not escape liability just because identity thieves are equally or more blameworthy. As discussed later, when individuals believe they are at risk of harm, it can have negative psychological effects. People respond differently when there is a risk of harm, as opposed to when they feel secure. As an illustration, many individuals will stick to the beaten path even though traveling via new terrain could lead them to their destination in less time. Lost time is an actual harm and the risk of the unknown is what led to the lost time here. In the consumer data breach context, having to take extra

78. *See* Nat'l Biscuit Co. v. Stroud, 106 S.E.2d 692 (N.C. 1959).

precautions because a data thief mishandled a victim's personal information is not speculative, unnecessary, or irrational. It is how the vast majority of people act in these situations, and it is in itself actual harm.

A consumer data breach creates a risk that was not present before. In demanding that a risk be likely to happen sooner rather than later in order to constitute an actual harm, the *Clapper* "certainly impending" standard and others disregard the actual harm that occurs simply by being subjected to a new risk. Courts should not even assess whether a risk is "certainly impending" or "substantial" enough. Instead, courts should only consider whether a new risk to a consumer has been created by the breach.

Simply put, a "certainly impending" standard—at least as it is applied to data breach cases—misunderstands that any risk of future harm is an actual harm incurred by consumers. *Clapper*'s "certainly impending" standard makes it almost impossible for plaintiffs to bring consumer data breach suits by forcing them to wait until the harm materializes into some tangible or physical harm. This flawed understanding of what constitutes a sufficient injury-in-fact creates a host of issues. Importantly, by forcing consumers to wait until harm materializes into a tangible or physical harm, injured consumers risk not being able to pursue recompense at all.

To illustrate this, "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[79] The words "fairly traceable" here serve to ensure that the causal connection between action and injury is sufficient.[80] If a consumer has to wait for a harm to "materialize," as each year passes, it becomes easier for defendant companies to argue that the harm is not a result of the data breach. In essence, the result means that consumers who are actually harmed by data breaches have no opportunity to seek reprieve. Take, for example, Target's 2013 consumer data breach, where tens of thousands of customers' account information details were taken.[81] When a data breach of that magnitude occurs, attackers likely cannot use the stolen information over the course of twenty-four hours. Depending on how much data is taken, it could be years before breached information is misused. If the Target consumers are forced to wait until they are able to prove that fraudulent identity theft has occurred or is otherwise

79. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (quoting *In re* Adobe Sys., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014)) (citation omitted).

80. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

81. Jim Finkle & Dhanya Skariachan, *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, REUTERS (Dec. 18, 2013, 4:05 PM), www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219.

"certainly impending," their case becomes infinitely harder to prove. In a situation like this, there is nothing to stop Target from claiming the breach was years ago and the information could have been obtained from any number of places. This is flawed justice as it lets companies avoid liability even though consumers were harmed as a direct result of their negligence in protecting private information. If the attackers do not use the obtained information for a decade or more, this does not discount the fact that it was because of Target's failure to protect consumer account information that the attackers had obtained the ability to use the information in the first place. What *Clapper*'s "certainly impending" standard does is discount the real harms that consumers incur, such that entities like Target are able to build defenses based on the amount of time that has passed between the breach and the fraudulent activity.

Additionally, a standard that forces consumers to wait until a risk is "certainly impending" or more tangible creates the possibility that people will not be able to seek redress for their injuries. This is especially true since many states have a seemingly short statute of limitations for identity theft cases.[82] For example, in California, the statute of limitations for identity theft cases is four years, and begins to run as soon as the crime is discovered.[83] To illustrate the gravity of the issue this creates, in *Storm*, it was ultimately determined that an estimated 233,000 consumers had their private information stolen by the breach.[84] As such, depending on the number of culprits, it is likely impossible to fraudulently use every individual consumer's data within a four year period.

Applying the *Clapper* standard to consumer data breach suits creates a very real threat by making it immensely difficult for consumers to bring suits within the limitations period. Under the *Clapper* standard, plaintiff consumers—when they are finally able to have standing at some point in the future—suffer the possibility of being barred by a short statute of limitations; all because *Clapper* made an allegation of increased risk of harm insufficient to satisfy the injury-in-fact standing requirement.

B. PRESENT INJURIES

In addition to a risk of future harm, consumer data breach victims suffer a number of actual present injuries such as presumed harm, financial harm, lost time, and psychological harm. These are actual harms that occur immediately upon a consumer data breach.

---

82. *See, e.g.*, CAL. PENAL CODE § 803, A.B. 1105 (West 2017); TEX. CODE CRIM. PRO. ANN. art. 12.01(3)(G) (West 2017).

83. CAL. PENAL CODE § 803, A.B. 1105 (West 2017).

84. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 363 (M.D. Pa. 2015).

1. Presumed Harm

Using a "certainly impending" standard to determine whether an alleged risk of future harm satisfies the injury-in-fact element of standing in consumer data breach suits further misses the point because even though an alleged risk of future harm in and of itself is an actual harm, we need not look that far. Even if there is no risk of future harm, the infringement of important legal rights presumes an actual harm.

The law recognizes this principle in a wide range of contexts, including battery, slander per se, and trespass. Take battery for instance. In *Leichtman v. WLW Jacor Communications, Inc.*, a talk show host lit a cigar and intentionally and repeatedly blew smoke in the face of an appearing guest who happened to be a nationally known antismoking advocate.[85] The guest sued for battery alleging that the host blowing smoke in his face was "for the purpose of causing physical discomfort, humiliation, and distress."[86] The court, in finding a valid claim, held that "[c]ontact which is offensive to a reasonable sense of personal dignity is offensive contact" for battery purposes.[87]

Additionally, certain language in and of itself is actionable as slander per se without proof of special damages.[88] A notable example is situations where a person is falsely accused of having committed a crime. Further still, courts overwhelmingly find standing in suits involving claims of intentional trespass even though there is generally no physical or noticeable harm involved. This is because "[t]he law infers some damage from every direct entry upon the land of another."[89] In *Jacque v. Steenberg Homes*, despite multiple objections from plaintiff homeowner, a mobile home selling company intentionally trespassed across private land.[90] Though traveling through plaintiff's field resulted in only nominal physical damages, the court found that a punitive damages award of $100,000 against the mobile home company was reasonable.[91] The court maintained that individuals have a "legal right to exclude others from private property" and that this right would be "hollow if the legal system provide[d] insufficient means to protect it."[92]

If not for the longstanding notion of protecting property interests, the court's holding in *Jacque* would be hard pressed to satisfy the standing requirements of Article III. If property interests were taken out of the equation, the only injury to plaintiff would have been a damaged

85. Leichtman v. WLW Jacor Commc'ns, Inc., 634 N.E.2d 697, 698 (Ohio Ct. App. 1994).
86. *Id.*
87. *Id.* at 699.
88. Gertz v. Robert Welch, 418 U.S. 323, 380 (1974).
89. Jacque v. Steenberg Homes, 563 N.W.2d 154, 160 (Wis. 1997).
90. *Id.* at 609.
91. *Id.* at 610.
92. *Id.* at 618.

ego. "I told them not to do it, and they did it anyway," is not a very compelling basis for standing purposes. The point here is not to discredit how the standing doctrine is currently applied to intentional trespass suits, but rather to embrace the analogy of the harm suffered in those cases to the harm suffered in consumer data breach suits. Similar to the harm incurred from an intentional trespass, individuals whose personal information is taken or used without permission immediately suffer an injury-in-fact.

Confidential details of a person's life can be obtained in a data breach. As shown throughout our nation's jurisprudence, privacy is a right ratified in a number of statutes.[93] One notable example is Article I, section 1 of California's Constitution, which states that the pursuit and obtainment of privacy is an inalienable right.[94] This right to privacy is not limited to states, as the right to privacy has been implied throughout the federal Constitution—most notably in the Fourth Amendment.[95] In the consumer data breach context, the federal Stored Communications Act prevents electronic communication providers from handing over a consumer's private information except for clearly defined exceptions.[96] This statute serves to show that consumers do not give up their property or privacy rights to a company just by using their services. And like battery, slander per se, and trespass, the harm that accrues may not be seen on the surface. When an individual's right to property or right to privacy has been infringed upon, there is harm regardless of whether the personal data has been used.

2. Actual Financial Harm

Knowing that a breach has occurred certainly causes time and expense because the victim must monitor and take steps to minimize the risk, such as reissuing credit cards, putting stop orders on payments, or fearing credit-report impacts. Take, for example, the risk of identity theft. It has been reported that "[t]he most commonly alleged injury in the wake of a data breach is an increased risk of future identity theft."[97] If a bank were to call a customer and say that the customer's credit card information had been stolen, but that the card has not yet been used anywhere, it is unlikely that the customer would just go about her day

93. *See, e.g.*, 18 U.S.C. § 2701 *et seq.* (2015).

94. CAL. CONST. art. I, § 1; *see also* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); FLA. CONST. art. I, § 23; MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed . . . .").

95. *See* Katz v. United States, 389 U.S. 347, 353 (1967); U.S. CONST. amend. IV.

96. 18 U.S.C. § 2701 *et seq.*

97. Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, BLOOMBERG (Nov. 9, 2015), https://www.bna.com/standing-data-breach-n57982063308 (citation omitted).

content with that knowledge. Indeed, the customer would be reasonably inclined to immediately cancel her credit card. And for the next few months, the customer likely would monitor her other accounts. This is because, when a data breach occurs, victims carry objectively reasonable beliefs that the information has landed in the wrong hands for purposes of misuse. Simply put, when it comes to consumer data breaches, there is nothing "speculative" about the incurred harm.

At the very least, victims of a data breach have to take the time to cancel and obtain new credit cards. This undeniably derails business dealings or time-sensitive purchases. Moreover, during this time, consumers likely are not able to use their accounts. Furthermore, it is likely that these consumers will have to change all of their online records of bank account or credit card information stored in the various websites we all use. The loss of time and money associated with a breach is an actual financial harm, and currently, courts are not recognizing this under *Clapper*.

3. Actual Psychological Harm

Even without the loss of time and money, there is a more basic harm—the invasion of privacy itself. On its own, a breach constitutes a sufficient harm for standing purposes because of the presumed psychological harms associated with it. There is actual harm at the breach stage, regardless of whether there is evidence that the obtained data was improperly "used." Though for the most part, psychological harm has already been a basis for satisfying the injury in fact element for consumer data breach suits, the importance of acknowledging this type of harm bears repeating. "If [a] plaintiff can show that there is a possibility that [a] defendant's conduct may have a future effect, even if the injury has not yet occurred, the court may hold that standing has been satisfied."[98]

To illustrate this point, in many states, "an entry alone is sufficient" for an act to be considered burglary.[99] Imagine coming home from work and finding your front door ajar. After either calling the police or bravely self-investigating the premises, you determine that a stranger has definitely been inside your home, but that it is unclear whether anything has actually been taken. At this moment, you are likely unnerved because someone has been inside your home without your permission; a home you originally thought of as secure. Thoughts encapsulate you. If this person was able to get into your home once, what is to stop them from obtaining access again? Better yet, did they take something that you just cannot pinpoint at this moment? For a court to say that you have not been

98. CHARLES A. WRIGHT ET AL., FED. PRAC. & PROC. CIV. § 1785.1 (3d ed. 2005).

99. People v. Davis, 18 Cal. 4th 712, 720–21 (Cal. 1998) (discussing the "entry" element under California's definition of burglary).

harmed in this hypothetical situation would be ludicrous.[100] Aside from the obvious psychological effects, your legal rights to privacy and property have been violated.

A 2015 study into the psychological trauma experienced by data breach victims found that identity theft victims often experience emotions similar to those of trauma survivors or persons who have been victims of a home invasion or assault.[101] As such, just as a court would not let a burglar go free just because a homeowner cannot prove something was taken, courts in consumer data breach suits should not dismiss cases by applying standards that are inadequate in the data breach context. Like seeing the front door of one's home ajar, the theft of personal data affects a person in a myriad of ways that are not simply tangible or seen on the surface.

It is objectively reasonable for a person to become distressed upon hearing that personal details about them have been breached. When a person's credit card is stolen, that person reasonably might respond by feeling worried, scared, angry, or stressed. Having to worry, because of a breach, that you might not be able to pay rent, or buy diapers, can seriously take a toll on a person's wellbeing. To put this in perspective, stress alone has been linked to the six leading causes of death: heart disease, cancer, lung ailments, accidents, cirrhosis of the liver and suicide.[102] It is not necessary to nitpick in determining what likelihood of psychological harm is sufficient for standing purposes, because as addressed previously, psychological harm is but one of many harms inflicted as a result of a data breach. Though the psychological effects can and likely will differ from individual to individual, this does not change the fact that there is always a possibility that a breach could negatively affect the mental health of a person. As such, psychological harm is an injury-in-fact that should be considered actual harm for standing purposes.

III. COUNTERARGUMENTS

One argument against this Note's proposed thesis is that the standing doctrine's purpose is to conserve judicial resources rather than broaden federal jurisdiction. The idea is that if plaintiffs are able to bring suits without showing that a sufficient injury has occurred, judicial resources will be spread too thin hearing claims that are miniscule,

100. For an infographic that shines a light on how victims of burglaries have been psychologically affected, see *The Psychological Effects of Burglary: Infographic*, VERISURE (June 11, 2016), blog.verisure.co.uk/psychological-effects-of-burglary.

101. EQUIFAX, A LASTING IMPACT: THE EMOTIONAL TOLL OF IDENTITY THEFT (2015), https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

102. Deborah S. Hartz-Seeley, *Chronic Stress Is Linked to the Six Leading Causes of Death*, MIAMI HERALD (Mar. 21, 2014, 11:53 AM), www.miamiherald.com/living/article1961770.html.

frivolous, or otherwise unwarranted. Courts want to reserve their resources for cases where there is truly a need for judicial facilitation. This Note respects this contention and does not attempt here to discredit the importance of preserving judicial resources. It is true that implementation of this proposed understanding of actual harm allows more consumers to seek redress. However, though more suits will be brought, this only means that justice is finally being afforded individuals who will now be able to have their cases heard on the merits. This Note does not suggest that all claims will be found to have merit once adjudicated. Rather, this Note simply calls for an understanding of injury-in-fact that will afford actually harmed victims of consumer data breaches the opportunity to finally be heard on the merits.

Opponents to this Note's proposed standing interpretation may argue that consumers currently seek redress from companies rather than the attackers who triggered the breach, and that this proposed standing definition would hurt defendant companies. It is true that this proposed understanding creates a burden on companies to constantly work to protect the confidential information of consumers. However, just because one party—here, the attackers—can be sued, does not mean that other culpable parties—such as the defendant companies—should not be held accountable for their own failures. Data collectors are under a legal obligation to keep customer data secure[103] and should be held accountable under the law when they fail to do so. Furthermore, this proposed understanding will force entities to actively seek out new ways to fully protect the private information provided by consumers.

To illustrate this point, one only need look back to the defendant entity in *Storm*. There, the breach occurred on April 7, 2014; the defendant entity did not discover the breach until 23 days after the breach occurred, and, more importantly, the defendant entity did not begin notifying plaintiff consumers until almost two weeks after the company discovered the breach.[104] Under the proposed interpretation of what constitutes an actual harm in consumer data breach suits outlined in this Note, the severe oversight and unacceptable delay in notification by defendant entity in *Storm* would likely not have occurred. Instead, defendant entities, knowing that a breach will give rise to litigation, will likely spend more time and resources monitoring and finding further ways to protect consumer information.

103. Depending on the type of entity and data, there are a number of regulations in place that require entities to provide reasonable security for sensitive information. *See, e.g.*, 15 U.S.C. § 1681 (2017) (referred to as the Fair Credit Reporting Act); 12 U.S.C. § 1828b (1999) (referred to as the Gramm-Leach-Bliley Act).

104. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 363 (M.D. Pa. 2015).

IV. REFORMING THE CASE LAW

As shown throughout this Note, courts are incorrectly applying *Clapper*'s "certainly impending" standard to the consumer data breach context. By applying this "certainly impending" standard, these courts are neglecting very real harms suffered by consumers. The new understanding of injury in consumer data breach cases proposed by this Note serves to prevent this continued injustice. To illustrate this new understanding's effect, the Second Circuit's opinion in *Whalen*, applying *Clapper*, held that credit-monitoring costs were not a sufficient harm.[105] Under this Note's proposed standing interpretation, the plaintiff in *Whalen* would not have had her case dismissed for lack of standing. Instead, the suit would have been adjudged on the merits of the case. Though it is uncertain whether a judge or jury would have ultimately found the defendant company liable, at least the plaintiff in *Whalen* would have had her day in court.

Likewise, in *Storm*, the Third Circuit—in adhering to the "certainly impending" standard of *Clapper*—expressly overlooked a plaintiff who had suffered very real harm by having to spend additional costs and hours commuting to a separate location for work.[106] There, the data breach made it so he could no longer use his government security clearance.[107] This injustice would not have occurred under the standing interpretation proposed by this Note. This is because in *Storm*, actual financial harm, psychological harm, and risk of future injury were all evident. Under the standard proposed by this Note, plaintiffs in *Storm* would have had their case heard and adjudged on the merits.

Though cases like *In re Adobe*, *Remijas*, and *Galaria* did not adhere to *Clapper*'s "certainly impending" standard, the courts there were only able to satisfy standing by finding impressive ways to distinguish *Clapper* from the consumer data breach context. Under this Note's theory of standing, these courts would not have had to work so hard. These courts all found standing to be satisfied by acknowledging some of the actual harms addressed in this Note, however, none of these courts went so far as to list as extensively the plethora of harms that should satisfy the injury-in-fact element of standing in the realm of consumer data breach cases. Instead of grasping to one type of harm as these cases did, this new understanding of what constitutes a sufficient injury-in-fact in consumer data breach suits comes with an arsenal of understood actual harms that will pass standing inspection.

If the nearsighted *Clapper* standard ceases to apply to consumer data breach suits, the question of standing in *Spokeo* will be an

105. Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015) (applying Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

106. *Storm*, 90 F. Supp. 3d at 363.

107. *Id.*

open-and-shut case upon its return to the Ninth Circuit. There, the court will find that Robins was sufficiently harmed when Spokeo listed false information about him. However, until the Supreme Court revisits the matter, the "certainly impending" standard will continue to create uncertainty as to whether a person who has actually been harmed will satisfy the injury-in-fact element of standing.

CONCLUSION

This Note illuminates how courts are currently misapplying one element of the standing doctrine—specifically the injury-in-fact element—to the particular context of consumer data breach suits. Further, this Note serves to call upon courts to re-evaluate what constitutes an actual harm in the consumer data breach context. Though this Note likely does not exhaust all of the actual harms incurred by consumers upon a data breach, it does serve to highlight certain common and undeniable actual harms. These harms include increased risk of future harm, presumed harm, financial harm associated with the breach itself, and psychological harm. This proposed interpretation acknowledges these very real harms, where current standards have failed to do so. The interpretation further serves to protect and compensate consumers who have suffered these real harms. Lastly, by placing the burden on companies, this proposed interpretation incentivizes these entities to take stronger measures to protect consumers, by constantly seeking better ways of preventing the theft of private information.